SECTION 28 50 00
SECURITY MANAGEMENT SYSTEM

PART 1 - GENERAL

1.1 SUMMARY

A. Section Includes

1. General description, functional requirements, operational characteristics, and products for the Security Management System (SMS).
2. Requirements for furnishing and installing a complete and operational SMS as specified herein and in accordance with the Contract drawings.

B. Related Sections

1. General provisions of the Contract including General and Supplementary Conditions.
2. Division 01 Sections, General Requirements.
3. Division 08 Section 08 71 00, Door Hardware.
4. Division 26 Section 26 05 00, Common Work Results for Electrical
5. Division 26 Section 26 05 19, Low Voltage Electrical Power Conductors and Cables.
6. Division 26 Section 26 05 29, Hangers and Supports for Electrical Systems
7. Division 26 Section 26 05 33, Raceway and Boxes for Electrical Systems.
8. Division 26 Section 26 05 36, Cable Trays for Electrical Systems.
9. Division 28 Section 28 05 00, Common Work Results for Electronic Safety and Security.
10. Division 28 Section 28 05 13, Conductors and Cables for Electronic Safety and Security.
11. Division 28 Section 28 05 26, Grounding and Bonding for Electronic Safety and Security.
12. Division 28 Section 28 05 53, Identification for Electronic Safety and Security.
13. Division 28 Section 28 08 00, Commissioning of Electronic Safety and Security.
14. Division 28 Section 28 10 00, Electronic Access Control and Intrusion Detection.
15. Division 28 Section 28 20 00, Electronic Surveillance.

1.2 REFERENCES

A. American National Standards Institute (ANSI)

1. ANSI C2 - National Electrical Safety Code

B. Conformite Europeenne (CE) where applicable

C. Federal Communications Commission (FCC)

1. Part 15, Radio Frequency Devices, Subpart J - Class A or B Computing Devices, as applicable

D. Federal Information Processing Standard (FIPS)

1. FIPS 140-2, Security Requirements for Cryptographic Modules

E. International Electrotechnical Commission (IEC)

1. IEC 529, Classification of Degrees of Protection by Enclosures

F. National Electrical Manufacturers Association (NEMA)

1. NEMA 250, Enclosures for Electrical Equipment

G. National Fire Protection Association (NFPA)

1. NFPA 70, National Electrical Code (NEC)

H. Underwriters' Laboratories (UL)

1. UL 294, Access Control Systems
2. UL 467, Grounding and Bonding Equipment
2. UL 634, Connectors and Switches for Use with Burglar-Alarm Systems
3. UL 1076, Proprietary Burglar-Alarm Units and Systems

I. Applicable Federal, state and local laws, regulations, ordinances and codes

1.3 DEFINITIONS/ACROMYNS

A. The following terms are defined for the purposes of this Section:

1. <u>Access Group</u>: A logical group of card readers (terminals) which may be connected to one or more controllers and that represent a collection of readers for which a particular entity may have access privileges.
2. <u>Access Mode</u>: The mode of operation in which the SMS shall only annunciate tamper and trouble conditions at a monitored point. Alarm conditions shall not be annunciated in this mode. This is referred to as "alarm shunting."
3. <u>Acknowledge</u>: The action taken by an SMS operator to indicate that he/she is aware of a specific alarm or tamper state.
4. <u>Advisory</u>: A message provided by the SMS to the operator to inform him/her of a condition as reported by the SMS.
5. <u>Alarm</u>: A change of state as detected by the SMS indicating that it has detected a condition that its sensors were designed to identify.
6. <u>Audit Trail</u>: A sequential record of system activity used to reconstruct and review a series of system events.
7. <u>Badge</u>: The physical card, carried by the cardholder to gain access at a door. Badges are also used to identify and track a cardholder in the system.
8. <u>Boolean</u>: An expression that results in a value of either TRUE or FALSE.
9. <u>Cardholder</u>: A person who is a member of the cardholder database that may have been issued a valid badge for identification, access, and tracking purposes.
10. <u>Card Reader</u>: A device usually located at access points, designed to decode the information contained on or within a badge identifier for the purposes of making an access decision or for identity verification.
11. <u>CE Mark</u>: European Union compliance symbol that indicates a product complies with all European directives and essential Harmonized Standards for health, safety, environment and consumer protection that may apply to that product.

12. CK7xx: This term refers to Johnson Controls CK7xx series controllers CK705, CK720, CK721 and CK721-A.
13. Clear: The action taken by an SMS operator to remove an alarm from the alarms queue after it has been acknowledged and, if required, responded to.
14. Controller: – This term refers to CK7xx series (CK705, CK720, CK721, and CK721-A), S321-IP, OSI, Isonas, HID, and Assa Abloy network panels or S321-DIN, S320, D6xx series (D620, D620-TIU, and D600 AP), and P900 serial panels. These connect to terminals and communicate with the Server. S320 and D6xx series panels are also called “legacy” panels.
15. Disable: A system command that intentionally places a device or system out of service, typically for maintenance.
16. Download: Refers to the transfer of system configuration information from the server to the memory of the controllers. This includes information such as badge records and access rights.
17. Dry Contact: A voltage free electrical contact.
18. Elevator/Cabinet Control: Elevators and cabinets have readers associated with a set of output points and an optional set of input points. The controller works with the elevator and cabinet manufacturer’s control system using output points to enable car-call buttons or unlock cabinet doors, and input points to monitor their status. The controller may grant access to a floor or cabinet door when a badge is presented at a reader installed at the elevator or cabinet. The elevator/cabinet access control allows the operator to assign cardholder access to various elevators, floors, cabinets, and doors in a facility using access group definition.
19. Events: Events are sequences of system commands or actions that may be activated at a predefined time or on an as-needed basis. Events can be activated and deactivated either manually or automatically.
20. Facility Code: A coded number, in addition to the individual card number stored within each card key, which uniquely identifies the facility at which the card is valid. This feature prevents cards from one facility being used at another facility with a similar access control system.
21. Field Devices – Represent reader interfaces, keypad/display modules, input points, and output relays.
22. Guard Tour: A sequence of transactions that, when performed within a specified time frame, ensures that the facility is being properly monitored by security personnel. The main purpose of a tour is to confirm and record that an area has been physically visited. It provides real time monitoring of guard activities - reporting if a guard arrives early or late to designated tour stations. Guard Tour stations can either be readers or input points. Tours can be selected randomly or may be specified at regular time intervals.
23. Hardware Modules: Refers to Johnson Controls modules I16, IO8, SI8, SIO8, I32O16, RDR2, RDR2S, RDR2S-A, and RDR8S which are installed in Johnson Control CK7xx controllers.
24. Input Point: Electrical contacts that open or close to inform the system of a change of state.
25. Legacy: Refers to S320 and D6xx series (D620, D620-TIU, and D600 AP) controllers’
26. Line Supervision: The process of monitoring an electrical circuit via electrical and software systems to verify the electrical integrity of the supervised circuit.
27. Loop: A number of terminals connected in series in a continuous circuit that starts and ends at the controller.

28. Monitoring: The process of maintaining a vigilant watch over a system element or point and taking appropriate action in response to system activity.
29. Offline: A condition in which a controller is not in communication with the server. In the offline mode, the controller continues to make access decisions and process alarms according to the information stored at its local database.
30. Output Point: Control external devices such as signals, relays, LEDs, control modules, etc.
31. Panel: See Controller.
32. Password: A combination of numbers and/or letters unique to each SMS operator.
33. Polling: Terminals are interrogated at regular intervals by the controller to establish and verify communications with other equipment and exchange data if necessary.
34. Port: A connection that provides a means of communication between devices.
35. Priority: The relative importance of system events.
36. Reset: A command or feedback signal that indicates that a monitored point has returned to its normal state having previously been at the alarm or trouble state.
37. Secure Mode: The normal state of an alarm input point. A change of state in this mode shall indicate an alarm, or that it has transferred to the trouble or tamper state.
38. Secured Area: A physical location within the facility to which access is controlled by one or more card readers.
39. Server: The main computer in the system. The server runs the SMS software, stores database information, and communicates with the field controllers and operator workstations.
40. Service: The process that performs specific system functions and operates in the background without user intervention.
41. Soft Alarm: Soft alarms and their addresses are created by the system during installation rather than hardwired to an actual input point.
42. Tamper: A condition within the circuitry of a monitored point, which indicates that the electrical integrity of that sensing circuit has been compromised.
43. Terminal: Terminals provide additional reader interfaces, input points, or output points to the SMS.
44. Time Zone: A user-defined period made up of days of the week and hours of the day during which events such as Valid Card Grants and Input/Output linking events may occur.
45. Transaction: Indicate some form of system activity. It may include items such as access requests and general system messages.
46. Trouble: A condition within the circuitry of a monitored point, which indicates that an equipment malfunction, single break, single fault, and/or a wire-to-wire short exists.
47. User-Definable: An attribute of an SMS function, which may be easily tailored by an operator without extensive computer programming knowledge or experience.
48. Workstation: A personal computer connected to the main Security Management System (SMS) server computer via local area network connections for the purpose of operating the system and responding to alarms.

B. The following acronyms are used in this Section:

AC	Alternating Current
ADA	Americans with Disabilities Act
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
AV	Audio Visual

BACnet	Building Automation and Control Network
BPI	Bits Per Inch
BPS	Bits Per Second
CCTV	Closed Circuit Television
CE	Conformite Europeenne (European Conformity)
CPU	Central Processing Unit
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DVR	Digital Video Recorder
FASC-N	Federal Agency Smart Credential Number
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard
FQRN	Fully Qualified Reference Name
GUI	Graphical User Interface
ID	Identification
IEC	International Electrotechnical Commission
In-X-It	Entry/Exit
I/O	Input/Output
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MIS	Management Information Systems
MSEA	Metasys system extended architecture
NEC	National Electrical Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association
ODBC	Open Database Connectivity
OPC	OLE for Process Control
PIN	Personal Identification Number
RFQ	Request for Quotation
RPC	Remote procedure call
SEIWG	Security Equipment Integration Working Group
SIA	Security Industry Association
SMS	Security Management System
SPDT	Single Pole, Double Throw
UDF	User Defined Field
UDP	User Datagram Protocol
UL	Underwriters Laboratories
URL	Uniform Resource Location
WAMS	Wireless Access Management Solutions
XML	Extensible Markup Language
3DES	Triple Data Encryption Standard

1.4 SYSTEM DESCRIPTION

A. The Security Management System (SMS) shall be capable of integrating multiple building functions including access control, alarm management, intrusion detection, video imaging and badging, and database partitioning and interfacing with closed circuit television (CCTV) monitors, digital video recording (DVR), and matrix switches and with intercom equipment. It shall also be capable of controlling multiple banks of elevators, as well as allowing cardholder information and queries from external system databases (MIS interface).

B. The SMS shall be, at the time of bid [*if required*], listed by Underwriters Laboratories for UL 294, Access Control Systems ,and UL 1076, Proprietary Burglar Alarm Systems. PCs and all controllers furnished with the SMS shall carry the UL 294 and UL 1076 labels as required. Bidders shall state their product is found on UL's certification web site and shall provide the corresponding URL.

C. The SMS shall be modular in nature and shall permit expansion in both capacity and functionality through the addition of controllers, card readers, workstations, or by increasing the number of cards and sensors.

D. The SMS shall incorporate the necessary hardware, software, and firmware to collect, transmit, and process alarm, tamper and trouble conditions, access requests, and advisories in accordance with the security procedures of the facility. The system shall control the flow of authorized personnel traffic through the secured areas of the facility.

E. The user interface at the SMS host computer (server) and at the operator workstation shall be a mouse-driven graphical user interface (GUI) allowing the user to open and work on multiple windows simultaneously.

1.5 SUBMITTALS

A. Submit in accordance with the provisions of Division 01 Section 01 33 00, Submittal Procedures.

B. Product Data: For each type of product furnished provide manufacturer and model number and associated manufacturer's catalog data sheet. Include rated capacities, operating characteristics, input power requirements, and furnished options and accessories. Reference each product to a location on the Contract Drawings.

C. Shop Drawings: System block diagram, system riser (signal and power), SMS equipment dimensions, layouts, and installation details, point-to-point wiring diagrams and termination details for all SMS devices, raceway locations, sizes, and type, and circuit schedule.

D. As-Built Drawings: Incorporate field changes (as-built notices) onto the original drawings after final installation is completed and accepted.

E. Manufacturer's User and Installation Manuals.

F. Test Data: Certified copies of test data for all tests performed on-site.

G. Course Outlines: For the end user programs. Each outline shall include the course duration, location, prerequisites, and a brief description of the subject matter.

1.6 QUALITY ASSURANCE

A. Manufacturer’s Qualifications: SMS manufacturer shall be an established organization with referenced and documented experience delivering and maintaining SMS of equal or higher sophistication and complexity as compared to the system detailed in this Section.

B. Bidder’s Qualifications: At the time of the bid, the bidder shall have satisfactorily completed projects of a similar size, scope, and complexity as the system detailed in this Section. The bidder shall furnish written proof of experience from three (3) references and proof of current accreditation or certification by the manufacturer for required training for sales or installation or service of the SMS and associated devices. The bidder shall also be a factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for the SMS and related systems under this Contract.

C. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.

1.7 DELIVERY, STORAGE, AND HANDLING

A. Upon receipt at the job site, all materials shall be checked to ensure that no damage occurred during shipping or handling.

B. Deliver, store, and handle materials, components, and equipment in manufacturer's protective packaging.

C. Store components and equipment in a secure temperature and humidity-controlled environment in original manufacturer's sealed containers.

1.8 PROJECT CONDITIONS

A. Environmental Conditions: SMS shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Indoor, Controlled Environment: SMS components installed in temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of [32-85}dry bulb and 20 to 90 percent relative humidity, non-condensing.
2. Indoor, Uncontrolled Environment: SMS components installed in non-temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of [32-85] dry bulb and 20 to 90 percent relative humidity, non-condensing.
3. Outdoor Environment: SMS components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions common for the project location including precipitation.

1.9 .SEQUENCING

A. Coordination: Coordinate work that must be performed in sequence with, or at the same time as, work in another Section.

1.10 WARRANTY

A. All equipment furnished under this contract shall be warranted for a period of thirty six (36) months from the date of final Owner acceptance of the system.

1. Respond to service requests on-site, if required.
2. Replace or repair defective components as required.

PART 2 – PRODUCTS

2.1 MANUFACTURERS

A. All access control hardware and software shall be of a single manufacturer including server system, controllers, and input and output terminal modules.

B. Base bid shall be Johnson Controls, Inc. **P2000** only. All alternate manufacturers seeking approval shall submit the following documentation to the Division Access Control and Intrusion Detection System Engineer for review thirty business days prior to bid.

1. Detailed bill of material for each piece of equipment submitted.
2. Manufacturer’s catalog cut sheet for each proposed piece of equipment.
3. Line-by-line typewritten compliance/non-compliance statement, comparing each requirement of the specification against verifiable performance specifications of the proposed product(s). This compliance statement shall be signed by an executive officer of the proposing company.

2.2 MATERIALS

A. Components selected for use in the SMS shall be of proven functional design, which shall be supported by documented performance data in two (2) other similar applications for at least one (1) year of continuous operation or subjected to suitable qualification testing as determined by the Owner.

B. SMS components shall be standard, off-the-shelf equipment of the latest model of current production at the time the system is proposed. The manufacturers of all equipment furnished shall have an established spare parts and maintenance network within the United States.

C. All materials and equipment of similar application cited shall be by the same manufacturer, unless noted herein. Like equipment modules shall be standardized to ensure interchangeability. To the maximum extent practical, equipment shall be provided as modular plug-in devices and shall be readily replaceable or interchangeable with identical devices.

2.3 SMS SOFTWARE

A. System Software

1. The server operating system shall be Microsoft Windows Server® 2008 R2 (64-bit) or Microsoft Windows Server 2008 (32-bit). It shall have multi-tasking and multi-user capability, and support workstations with Windows XP® (32-bit and 64-bit) operating system.
2. The system database shall be Windows SQL Server™ 2008 R2.
3. The SMS software features shall be fully documented in the form of a complete User's Manual including operation and installation sections, and a detailed description of the major SMS functions.
4. The software shall have an installed capacity to accommodate the following at a minimum:
    a. A central database on the server able to support up to 200,000 badges maximum.
    b. Unlimited number of access groups.
    c. Up to 16,000 2-state alarm input points, or up to 8,000 4-state alarm input points (or any combination in between).
    d. Up to 40 operator workstation terminals connected to a server via an Ethernet TCP/IP network.
    e. Central online data storage of 500,000 historical transactions, expandable (as system resources allow), with local panel storage capability of up to 50,000 events.
    f. 256 levels of alarm priority.
    g. A minimum of ten (10) individual badge identifier numbers per cardholder. Each badge shall be tracked separately.
    h. 255 issue levels per card, only one of which shall be active at any given time.
    i. Unlimited number of user-defined fields. The SMS shall be capable of reporting on any or all of the fields. Each field may be defined by the user as either alphanumeric text, numeric, date, or Boolean.
5. The SMS shall be capable of partitioning (segmenting) the database which must include, but is not limited to, the following items:
    - Cardholders
    - Badges
    - Time Zones
    - Holidays
    - Access Groups
    - Panels
    - Reader/Terminals
    - Workstations

B. Operational Requirements

1. General: The SMS shall operate in client-server architecture. Any SMS software and firmware required for the following system functions shall be fully tested with the existing SMS application software. Custom software including "ladder logic programming" and other custom application programming intended to provide the following features are unacceptable.
2. Database Management: The system shall create and maintain a master database of all cardholder and configuration (hardware devices) records, as well as system activity (audit, alarm, and transaction history) for all connected points.
3. Audit Trail: The SMS shall maintain an audit trail file of operator activity, and provide the ability to generate a report by operator, time and date, and type of activity. The system shall allow the operator to direct the audit trail report to screen, printer, or file. The audit trail feature shall record operator activity associated with:
    - Users
    - Partitions
    - Elevator parameters, including configuration, floor names, floor

- Badges, badge layouts, badge fields, badge IDs, badge reason, badge encoding, identifier purpose, automatic badge numbers, setup
- Cardholders, entity categories and entity groups
- Field devices such as panels, terminals, terminal groups, input points and groups, output points and groups
- Access groups
- Holidays, time zones, panel holidays and panel time zones
- Access templates
- Companies and Departments
- Soft alarms
- Site Parameters
- Workstations
- User Defined Fields
- Events
- Panel card event
- Alarms, alarm filters, alarm history, alarm response text, alarm colors, alarm instructions, alarm categories, alarm options
- Message forwarding
- Permission groups
- Panel relays
- Reports
- MIS Interface
- Image recall filters
- Counters
- BACnet elements such as action interlocks
- External IP configuration
- Guard Tour definition, station definition and guard tour history transactions
- Loop configuration
- Enterprise Sites and Enterprise Parameters
- Web Access configuration
- Integration Component
- Assa Abloy facility and badge format

masks, floor groups

- Cabinet parameters, including configuration, door names, door masks, door groups
- Area and area control layouts
- Muster zones and muster history transactions
- CCTV elements, including server, switch, tour, alarm, macro, system auxiliary, monitor, sequence, camera, preset, pattern, and camera auxiliary
- Maps and map icon sets
- Enable codes
- P900 elements such as flags, counters, trigger events, trigger links, system parameters, sequence files
- Air Crew PIN number
- Remote Server
- Message filters and message filter groups
- Local Site
- Service Startup Configuration
- Application
- Panel Card Format
- Security Level Range
- Audit
- Transaction History
- Redundancy
- Intercom interface, exchanges and stations
- Audio Visual (AV) elements such as site, camera, monitor, preset, input to camera, dry contact
- Request Approvers
- FASC-N CCC
- SIA Device
- MSEA graphics, registration and partition
- OSI facility
- SIA device
- Software Update
- HID Facility
- Intrusion
- Kone IP Elevator

4. Online Help System: The SMS shall provide online help, which shall be available at anytime from any active screen by pressing <F1>.

5. Online Tutorial: The SMS shall provide an online tutorial program with an overview of the security system's major features and options, as well as system configuration, installation, and troubleshooting tips. The tutorial program shall be available from the Help option in the SMS menu bar. The modular design shall enable navigation to all or specific tutorial topics. The tutorial shall introduce topics and sub-topics which are discussed through Flash presentations that provide audio narration, with matching text if desired, to guide users on how to make the most of SMS's main popular features. Software screenshots shall be used to walk the user through actual configuration and installation steps.
6. Operator Access: The SMS software shall limit system access only to authorized operators. Authorized operators shall be identified by their unique combination of user name and password. The SMS shall assign authorized operators with system privileges and characteristics that allow them to perform various system functions and shall provide for automatic log off due to user inactivity. Operator records shall be created for each person who will operate the Server or a workstation in the SMS and shall consist of:
   a. Login name and password
   b. Parameters to provide added security by requiring operators to enter their password when performing certain system-critical functions. The SMS shall also allow passwords to be validated by network directory services.
   c. Assignment to menu permission groups. The SMS shall assign to the operator menu permissions that define the system elements to which the operator can access...
   d. Assignment to user-defined fields. The SMS shall provide a tool to restrict operators from viewing certain user-defined fields.
   e. Assignment to message processing groups. The SMS shall assign the operator with message filters to define which messages the operator can see.
   f. Assignment to alarm processing groups. The SMS shall assign the operator with message filters to define which alarms the operator can process.
   g. Assignment to alarm processing groups. The SMS shall assign the operator with message filters to define which alarms the operator can process (acknowledge, respond, complete, etc.), and if the operator can process more than one alarm at a time.
7. Password Controls: The SMS shall provide password controls to determine how operators can access the system. The system administrator shall be able to define a number of parameters to set up strong passwords, passwords that are hard to break such as password validation to provide periodical password changes, minimum password length, number of letters (uppercase and lowercase) or numerals required in a password. Stored passwords shall be encrypted. Additionally, the software shall disable user access on multiple invalid logon attempts.
   a. The SMS shall also allow passwords to be authenticated against Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) to allow operator passwords to be validated by the network directory service.
8. Workstation Control: The SMS shall allow workstations to be assigned a name, and to have the following capabilities:
   a. Be identified as either workstation only, or workstation/video badging.
   b. Have a time zone to define the period to be in use.
   c. Assign message filtering to define the messages that can be transmitted to the workstation.
   d. Have an enable/disable toggle button to allow or deny operator logon at the workstation.
   e. Have a location name to describe the area where the workstation is to be found.

    f. Alarm monitor selection option to define whether or not the Alarm Monitor window shall display at the workstation after logging on.

9. Workstation Monitoring: The SMS shall provide an application to display workstation status information, including the workstation's current SMS software version installed. Operators with proper permissions shall be able to monitor which users are currently logged on at what workstations, and at what time they logged on. Operators shall have the option of logging off a workstation that is currently logged on.
10. Software Updates: The SMS shall support the automatic distribution of software updates to workstations in the SMS. Administrators shall configure the server to force update all workstations in the system or allow workstation operators to accept or deny the update when logging into the system. The Automatic Update feature shall eliminate the need to manually update each workstation when a new SMS software version or service pack is released. The server shall track each software update installed, providing detailed information such as the version number, service pack number, installation date, the location of installation files, and whether the update is optional or required.
11. Communication Modes: The SMS shall communicate with controllers that provide reader interfaces, input points, or output relays. Communication shall be bi-directional, some messages shall be sent from the server to the field controllers, other messages shall be sent from the controllers to the server, and then can be distributed within the system (e.g. workstations). The SMS shall provide the following three operating modes:
    a. **Local** – All access decisions shall be made by the controllers. This eliminates the need for panels to communicate with the server every time an access request is presented at a reader. Local mode provides the best overall system capability; however, access will be denied to those badges not stored in the controller memory.
    b. **Central** – This mode is useful when assigning access restrictions on a global scale (throughout the entire system). All access requests shall be forwarded to the server for an access grant or deny decision. Central mode has the most impact on system performance (the slowest), and should be used only when necessary.
    c. **Shared** – Access decisions shall be made either at the controller level or by the server. Controllers will first search for a badge in their memory, as in Local mode. If a badge's record is not found at the controller level, the access request is then forwarded to the server, as in Central mode. Shared mode is useful when a controller's badge capacity is exceeded.
12. Event and Transaction History: The SMS shall maintain a record of all alarms, card transactions, and system exceptions, and provide a means for users to access this information. This log can either be viewed in real-time or by printed report.
13. Localization (Optional): The SMS shall provide an internationalized framework to assist companies and users to work effectively in their native language. All text in the SMS menus, dialogs, and prompts shall display in the language selected.
14. Holidays: The SMS shall allow the definition of unlimited holiday dates that can be used throughout the system to allow or restrict access in the facility during the defined holiday date.
15. Time Zones: The SMS shall allow the definition of unlimited periods (time zones), during which a reader, badge, alarm point, or other system component or feature is active or inactive. Each time zone shall have the following identification and configuration parameters:
    a. Alphanumeric name.
    b. Alphanumeric description.

c. A set of enable and disable times applied to days of the week and three defined holidays.

16. Input Point Monitoring: The SMS shall collect and process status information from all monitored points.
17. Alarm Annunciation: The SMS shall audibly and visually annunciate all alarms, advisories, and tamper and trouble conditions.
18. Input Point Supervision: The SMS shall electrically supervise all 2-state and 4-state input point circuits as specified or shown on the drawings.
19. Alarm Input Point Reporting Delay: The SMS shall allow the operator to apply an input point reporting delay period from 0-60 seconds for each input point terminal. The default setting for each input point reporting delay shall be zero seconds.
20. Alarm Input Point Suppression: The SMS shall provide an alarm input point suppression facility such that the operator may define a time zone suppression period for each individual input point. Alarm conditions for suppressed input points shall not be recorded or archived by the system; however trouble conditions will be recorded.
21. Alarm Handling: The alarm handling portion of the SMS shall provide the following:
    a. Alarm monitoring window – displays the total number of alarms in the queue and the number of alarms pending. Alarms can be sorted by column.
    b. Users shall be able to see the location of an alarm on a map by selecting an alarm from the Alarm Monitor window.
    c. For alarm messages that are associated with a camera, users shall be able to display live or stored video associated with the alarm.
    d. User-definable alarm message/instructions description – allows the user to assign an alarm message/instruction to input points and other applications.
    e. Alarm message “pick list” – all alarm message names and associated descriptions display in the form of a pick list from which the user may select an appropriate alarm name and message.
    f. Alarm input points – the system supports up to 17,000 alarm-input points.
    g. Alarm input point maintenance – allows the operator to ‘Add’, ‘Edit’, or ‘Delete’ an alarm input point. The ‘Delete’ option requires user confirmation. All maintenance functions are logged to the audit trail and archived to the hard disk of the server.
    h. The system shall support both 2-state and 4-state alarm input point monitoring as called for in this specification or as shown on the drawings.
    i. Alarm priority – an alarm priority queue from 0-255. Individual wave sound assignment will be based on alarm priority.
    j. Alarm pop-up – alarm inputs that are designated, as “pop-up” by the operator shall take priority over any active non-alarm window. If the operator is viewing a non-alarm window when a pop-up alarm occurs, the alarm queue window shall be automatically placed on top of all other windows to allow the operator to respond to the alarm condition.
    k. Alarm instruction display – a window containing up to ten lines of user-defined instructions, which indicate to the operator how to respond to the selected alarm.
    l. Alarm condition history display – a window displaying the alarm history, together with a time and date stamp of each condition.
    m. Alarm response entry – a window in which the operator may enter free-form text (up to 255 characters) describing how he/she responded to a given alarm.
    n. The operator shall be able to select from a list of predefined response descriptions.
    o. The operator shall be able to activate events from the alarm monitor to trigger actions associated with the alarm.

p. The alarm instruction display, alarm condition history display, and the alarm response entry box shall all be part of one summary window. Separate windows or applications to support any of these three functions are unacceptable.

q. Alarm colors – the operator shall be able to recognize specific alarms by the color assigned to each. Color assignment is based on alarm priority and alarm state.

r. Alarm categories – every alarm in the system shall belong to at least one alarm category, but can also be assigned to multiple alarm categories. The operator shall be able to define an unlimited tree of alarm categories, each with its own set of alarm options.

s. Alarm escalation – the SMS shall constantly monitor all generated alarms that have the escalation option enabled. The alarm escalation feature shall provide for two different conditions when an alarm may be escalated: (1) if an alarm is generated for a specific alarm category and there are currently no operators logged on to the system that have privileges to receive alarms for that category and (2) if an alarm is generated and remains pending for the configured escalation timeout period. If either of these conditions occurs, that alarm shall be regenerated with an elevated escalation level. The escalation level shall be incremented by the configured escalation increment value. This process may be repeated multiple times until a high enough escalation level is reached that matches the privileges of a currently logged on operator. If no operators are logged on to the system, the alarm shall be regenerated until the maximum escalation level is reached, and then no further action will be taken. After an escalated alarm has been completed, the next occurrence of that alarm shall be created with no escalation level.

t. Alarm printing – the operator shall have the option of printing a list with all alarms in the queue or only print a list of the alarms that are visible in the alarm monitor list box.

u. Remote alarm monitoring – the SMS shall be configured to receive alarm messages from remote sites, allowing operators to simultaneously monitor alarms locally and at multiple remote sites.

v. Alarm monitoring using SIA interface – the SMS shall interface with a Radionics security receiver/controller to receive alarm messages using the SIA standard message format.

22. Global In-X-It Tracking: The SMS shall send messages to the real time list to report global entry/exit violations. A global entry/exit violation occurs when access is granted after presenting a valid badge at, for example an entry reader and then that badge is presented again at another entry reader, despite the requirement to badge at entry and exit readers alternately.

23. Enhanced Local Global Entry/Exit Synchronization: The SMS Entry-Exit enforcement application shall include system wide readers. This feature shall allow synchronization of badge status across multiple panels.

24. Badge Trace Alarms for Granted or Denied Access: The SMS shall generate alarms when a badge with the Trace flag set is granted or denied access at any reader in the system.

25. Special Access: The SMS shall provide special access that allows setting up a door's access time to be different, to satisfy the requirements for assisted access according to ADA (Americans with Disabilities Act). The system shall provide up to three special access flags, and then assign them to a cardholder that requires special access at a door. Additionally, the SMS shall provide the activation of an ADA relay in conjunction with the granting of assisted access.

26. Port Configuration: The SMS shall allow changing default port values that are assigned to system applications during software installation. Some of these values must match the values configured at the panel.
27. Smart Card Management: The SMS shall support the Federal Government smart card encoding protocol. All encoded badges shall include FASC-N (Federal Agency Smart Credential Number) data fields. The SMS shall allow the option of defining FASC-N badges, normal badges, or both as the badge type to be used throughout the facility.
28. Email Settings: The SMS shall allow setting e-mail accounts that shall be used to send e-mail messages as event actions, and where automatic error return could be sent. Settings shall include the domain name sent with the SMTP “Hello” command, a return address, and SMTP server name.
29. External Event Triggers: The SMS shall allow external inputs to be used as event trigger conditions. These external inputs can be in the form of an RS232 serial message or a TCP/IP message; an ASCII file or a database write. These inputs shall allow external software or hardware systems to send a message to the SMS, which will trigger a Host event that will in turn generate an alarm or other event action.
30. XML RPC Settings: The SMS shall provide a tool to configure communications with an external device using the XML RPC protocol. Configuration shall include password encryption mode selection and an enable/disable toggle button to allow or deny the SMS to accept XML RPC commands from any IP address. If disable, the SMS shall only accept XML RPC commands from IP addresses defined using the External IP Edit tool.
31. External IP Configuration: The SMS shall allow defining a computer or device to accept messages from external devices. The operator shall also be able to define a computer or device from which the SMS shall not accept external messages. If the SMS receives an external message from a source that is not configured, the SMS shall log an error message and not process the message.
32. Current Loop Configuration: Serial panels shall be configured for loop communication. The SMS server shall contact each serial panel in the loop for information. Each panel shall be polled in sequence in either forward or reverse direction. If communication is interrupted on one direction, the Server shall poll in the opposite direction to ensure that all panels are polled. The loop system shall support up to 32 loops with up to 30 panels per loop.
33. Dual Ethernet Interface: The SMS shall provide an alternate panel connection to configure panels that have a second network connection through a Dual Ethernet interface. Dual Ethernet allows the alternate connection to take over the communications if the primary connection fails.
34. Exempt from Archiving to Flash: The SMS shall provide the option of not saving the following databases to Flash during a Write-Flash operation:
    a. Badge
    b. Access Groups (including elevator access groups)
    c. Configuration: (including the Panel Configuration databases such as Elevator Configuration, Terminal, Input, Output, Time Zones, Holidays, Soft Alarms, and Card Events)
35. Backup Database to Flash Interval: The SMS shall allow entering the time interval (in hours) to schedule automatic backup of the panel database to flash memory. The default backup period shall be once every 24 hours. A backup period of 0 hours shall disable automatic database backups to flash memory.
36. Controller Configuration: Each controller shall be set up and configured using the SMS software using the following identification and operating parameters:
    a. Alphanumeric name.

b. **IP Address** – to match the IP address set up at the panel.

c. **Panel Poll Interval** – to define the number of days, hours, minutes, and/or seconds to set up the maximum time that the panel should be without contact with the SMS Server. This value shall be downloaded to the panel.

d. **Host Poll Timeout** – to define the number of days, hours, minutes, and/or seconds that the SMS Server will wait without receiving a poll, until it declares the panel down.

e. **History Settings** – to define how the panel uploads data to the SMS Server, and how long the panel retains data in the transaction database before older data is deleted.

f. **Time Offset** – to enable a time offset if the panel is in a different geographical time zone from the SMS Server.

g. **Timezone Checking** – to define if the panel is to check for valid reader and badge time zones, badge access requests, PIN code suppression, and upload suppression during the assigned time zones. If none is defined, badge access decisions shall be made on the basis of valid badge and valid access group parameters only.

37. Encryption: The SMS software shall secure every message to and from the controller, using Advanced Encryption Standard (AES) to protect the SMS from unauthorized sources. The SMS encryption shall be implemented using Federal Information Processing Standards (FIPS) 140-2, validated, and certified, cryptographic module, from Microsoft. Also, all real time messages from the SMS server to services and workstations shall be encrypted using AES with a 256-bit key.
38. Peer to Peer Badge Sync: The SMS shall provide an option to have entry/exit privileges enforced on reader terminals connected to different panels. This feature shall allow a panel to broadcast the entry/exit status of a badge to multiple panels, via User Datagram Protocol (UDP). The entry/exit zone shall span across multiple panels within the same subnet or across multiple subnets using a properly configured multicast router.
39. Input Suppression Messages: The SMS shall allow input points that enter suppression to be reported as being suppressed. When the input is no longer suppressed, the current input point state is reported.
40. In-X-It (Entry/Exit) Control: The SMS shall support the capability to control a card's entry into or exit from an area based on the previous transaction status of the card. An alarm may be generated if the cardholder violates the In-X-It conditions.
41. Alarm Shunt Only for Auxiliary Access: The Aux-Access Input Point on the terminal shall suppress only the Door Open Alarm. When not selected, the Aux-Access Input Point on the terminal shall perform an access grant.
42. Facility Code Only when Offline: The terminal shall accept any badge with the correct facility code when the terminal is offline from the panel.
43. PIN Required when Offline: An algorithmic PIN number shall be required for badge acceptance if the terminal goes offline.
44. Allow PIN after Badge: The cardholder shall enter the PIN number after presenting the badge instead of before presenting the badge.
45. Access Grant Message on Door Open Only: Access grant messages shall be generated when the cardholder swipes the badge and opens the door.
46. Anti-Tailgate Control: The SMS shall provide the capability to prevent more than one person accessing a controlled area because of a single card transaction.
47. Re-lock on Door Open: Normally the Anti-Tailgate and Timed Override/Anti Tailgate options cancel both access time and shunt time when the door closes. Enabling the Re-lock on Door Open option shall modify the anti-tailgate feature to lock the strike when the door opens, for example to avoid excessive wear of the electrical equipment. The shunt time shall still be cancelled when the door closes.

48. No Green Light On Aux Access: The SMS shall provide this option to disable the green light displayed on AUX access.
49. Deny if Door Open: The SMS shall provide the option of generating access denied messages when cardholders swipe their badges at opened doors.
50. Anti-Passback Control: The SMS shall provide the capability to prevent more than one person from gaining access to a controlled area by recognizing when a cardholder with access privileges attempts to pass their card back to another person. If so programmed, an alarm may be generated if the cardholder violates the anti-passback rules. It shall be possible to define which readers are subject to anti-passback rules on an individual basis.
51. PIN Plus 1 Duress: The SMS shall provide this option to enable a duress alarm to be generated when a cardholder adds 1 to the last digit of the PIN code. When this option is enabled, the 9 does not create a duress alarm. If the last digit of the PIN code is a 9, then the user substitutes a 0 for the 9 and this will trigger the duress alarm.
52. Star Feature: The SMS shall provide the Star Feature to enable cardholders to press the star (*) key at the keypad plus a feature number, to activate some of the panel’s functions that are normally invoked from keypads that contain the A, B, C or D keys. The (#) key acts as the Enter key, it wraps-up the previously entered keys and starts the processing of the key sequence. It also clears the keypad buffer for the next command to be entered. The (*) key starts the feature selection process. Once pressed, the cardholder can activate one of the following features:
    0 = Local Override, followed by number of minutes
    1 = Enable event, followed by event number
    4 = Disable event, followed by event number
    * = Clear the keypad buffer (works independently of the Star Feature setting)
53. BQT Reader with LCD: The SMS shall enable the LCD display of the following messages (arranged from highest to lowest initial priority):
    - Reader Offline
    - Access Granted
    - Access Denied
    - Enter PIN Code
    - Enter Shunt Time
    - Shunt Time Warning
    - Present Card

54. Duress Processing: The SMS shall permit cardholders to force a soft alarm to indicate that they are requesting access to an area under force or duress. In the event of such a situation, the cardholder will be granted access and an alarm will be generated.
55. Override Reset Threat Level: The SMS shall allow readers to be configured with an Override Reset Threat Level ranging between 0 and 99. A value of 0 disables the “Override Reset” feature; a value between 1 and 99 invokes the following behavior:
    a. Whenever a terminal’s Security Level reaches or exceeds the terminal’s Override Reset Threat Level, all time zone based overrides, host initiated overrides, and cardholder overrides are immediately disabled. Subsequent attempts to invoke host initiated overrides or cardholder overrides will be denied.
    b. Once a terminal’s Security Level drops below the terminal’s Override Reset Threat Level, the time zone based override is restored immediately. Host initiated overrides and cardholder overrides are not automatically restored, but subsequent attempts to invoke host initiated overrides or cardholder overrides will be granted, provided the configuration allows these overrides.
56. N-Man Rule: The SMS shall provide additional security measures for specific access-controlled readers using the N-Man rule function. The N-Man Rule is based in a team of cardholders who must present their badge as a group within a defined period of time in

order to gain access at an N-Man Rule defined reader. For this option to work, the terminals are required to operate in Central mode. The SMS shall enable visitors to gain access at an N-Man rule defined reader, as long as their sponsor presents the badge after the visitor.

57. Control Points: The SMS shall allow input points to be defined as control points when used in input/output linking and event processing sequences of operation. Control points shall not enter the alarm queue and shall not require that an operator acknowledge them when they change state. The control point activity shall, however, be automatically logged to the history file.
58. Air Crew PIN: The SMS shall allow the definition of air crew personal identification numbers (PIN). Once the Air Crew PIN numbers are defined, a system administrator shall enable or disable the Air Crew PIN feature. When this feature is enabled, entering the assigned Air Crew PIN number shall allow access at the door. Air Crew PIN numbers shall be assigned to a group of people or shall be assigned individually to an Air Crew member with different access needs. Presenting a badge shall not be required when using the Air Crew PIN Number feature.
59. Custom Card Formats: The SMS shall support up to eight custom card formats that can be downloaded to the panels. Upon selection, custom card files shall be stored in a separate database table. Once the selected card formats have been compiled, they will be available for selection.
60. Add Hardware Module: The SMS shall provide a wizard style interface that simplifies the process of adding new modules to the panels. The wizard shall ask the operator some basic configuration information specific to the module being added and automatically adds the necessary configuration items (terminals, input points, and output points) to the SMS system.
61. Elevator Access Control: The SMS shall communicate with compatible elevator equipment to provide cardholders access to various floors in a facility. The elevator access control feature shall allow up to 16 elevators per controller, and a maximum of 128 floors. History of elevator activity shall be maintained in electronic or printed form. The SMS shall support the following elevator interface configurations:
    a. D620-ECG Elevator Mode
    b. KONE™ High Level Integration Elevator Support
    c. KONE IP High Level Integration Elevator Support
    d. Otis® EMS-Security/BMS Elevator Support
    e. Otis Compass Elevator Support
    f. Low Level Elevator Support
    g. High Level Elevator Support
62. Cabinet Access Control: The SMS shall provide protection to sensitive information by monitoring and controlling access to files and equipment contained in a cabinet. The SMS shall allow a single reader to provide access to up to 32 cabinets. Cabinet readers shall be associated with a set of output points to unlock cabinet doors and an optional set of input points to monitor the status of cabinet doors.
63. Message Filtering/Routing: The SMS shall control the types of messages that are transmitted and received to and from local or remote systems, thereby reducing network traffic by transmitting and receiving only messages that pass a filter criterion. Filtering shall be applied based on the operator logged on to the workstation. Filtering criteria shall include alarm or message type and subtype, site name, operator name, partition, item name, query string, alarm category name, and priority and alarm escalation ranges.

a. To allow the transfer of alarm and transaction messages between the SMS servers located at different sites, a remote server application shall be properly configured at each remote site that wishes to transmit and receive alarm and transaction messages. The setup shall include the name, IP address, listener port number, and protocol (binary, HTTP Post XML, and XML) of the remote site; the type of messages that shall be forwarded and at what times; message queue parameters, and parameters specific to individual transmission sessions.

64. Access Templates: The SMS shall provide a tool for speeding the assignment of access options to large groups of cardholders that need the same access privileges. The SMS shall set all access options at once by defining an access template that contains preset badge options, access groups, and time zones, and shall override any settings already defined for each individual badge. Badge options could be edited individually after the template is applied.

65. Required Cardholder Fields: The SMS shall provide the definition of required cardholder fields, which must be completed before a cardholder record is saved. The Cardholder application shall display an asterisk (*) next to a field to indicate a required field. If a required field is left empty, the system shall display a warning message to indicate that a required field has not been completed.

66. User-Defined Cardholder Database Fields: The SMS shall support an unlimited number of user-defined data fields, which shall be used to store additional cardholder information. Each field shall be defined by the following parameters:
    a. UDF name.
    b. UDF type: Text, Numeric, Date, Boolean or Selection. A Selection field shall allow the definition of set values to choose from a drop-down list.
    c. Whether the field is a required field, that way the field shall always be completed.
    d. A width field to define the number of characters allowed.
    e. An option for converting a Text type field into a Selection type field. All previously values defined for the Text field shall be converted to set values to choose from a drop-down list.

67. Cardholder Definition: The SMS shall allow the definition of cardholder records for every person who needs access to a facility. Once the cardholder records are defined, the SMS shall be able to grant or deny the cardholder access to defined areas of the facility based on the cardholder’s access privileges. Cardholder records shall be defined by the following identification and operating parameters:
    a. Cardholder name (first, middle, last)
    b. Cardholder type (regular or visitor)
    c. Cardholder ID (the SMS shall provide a tool to automatically generate cardholder ID numbers)
    d. Cardholder portrait
    e. Cardholder address
    f. Cardholder phone number and extension number
    g. Validation period using start and end dates
    h. Department and Company information
    i. Web access permissions and password to log on to Web Access.
    j. Email address
    k. Cardholder journal. Journal entries shall supplement cardholder information by storing notes associated with each cardholder. The Journal shall display the date and time when the journal was entered, the name of the operator who last edited the journal,

the date and time the journal was last edited, and whether there is an attachment file associated with the journal entry.

l. Whether the cardholder is assigned with Guard privileges to participate in guard tour operations

m. Unlimited number of user-defined cardholder fields. The SMS shall use these fields in filtering reports

The Cardholder application shall select automatically the name of a newly added cardholder in the list of cardholders. The application shall also allow the display of cardholder badge transaction history and shall provide a search tool to easily find cardholder records in the database.

68. Badge Definition: The SMS shall allow cardholders to be defined by any of the following badge identification and operating parameters on a per badge basis:

a. Badge number assignment (the SMS shall provide a tool to automatically generate badge numbers)

b. Badge type (access or identification)

c. Badge description

d. Issue level (0-255), only one per badge

e. Badge facility code

f. Reason for issuing a badge (selected from a predefined list)

g. Badge purpose to specify the badge's intention (selected from a predefined list)

h. Badge format

i. Validation period using start and end date and time

j. Executive privilege enabled or disabled

k. Active/Disable badge toggle button

l. Trace option to enable or disable cardholder movement throughout the facility

m. Override enabled or disabled

n. PIN code (4 or 5 digits)

o. Badge event privilege level (0-7)

p. Security level (0-99)

q. Special access privileges (to satisfy requirements for assisted access according to ADA)

r. Assign a minimum number of 10 badges per Cardholder

s. Assign 32 predefined Access Groups and Time zones per badge

t. Assign personalized access group for each cardholder

u. Duplicate feature to create any number of badges for a cardholder that will use the current badge information; however each badge must have a unique number.

v. Access rights template selection list of predefined badge access options

w. Floor assignment for cardholders that need access to Otis Compass elevators

69. Temporary Access Feature: The SMS shall assign "temporary access" to any valid access group for each individual badge. Temporary access shall be defined on a selected date and time, which shall grant the cardholder permission for limited access within the normal time zone. Temporary access shall be based on the following parameters:

a. **Start** – specifies the date and time when permission for access shall be granted. If this is not specified then access is granted immediately.

b. **Void** – specifies the stopping date and time when permission for access expires.

70. Visitor Definition: The SMS shall allow an easier and faster way to enter visitor and badge information, by allowing authorized operators to enter visitor and badge data using a single user interface. Prior to a visitor's arrival, the operator shall be able to enter the appropriate visitor data into the system, shall assign a visitor sponsor, shall enter the date

and time period of the scheduled visit, and shall assign access privileges using Access Templates, subsequently and from the same screen, the visitor badge shall be printed.

71. Bulk Badge Change: The SMS shall enable operators to change badge parameters across multiple records in a single operation. Operators shall save time by modifying multiple records at once, improve the accuracy from single record editing, and avoid the hassle of updating badge records one entry at a time. In addition, they shall be able to delete multiple badges and/or associated cardholder records at the same time. The following operations shall be available:
    - Add Access Group
    - Apply Access Template
    - Delete Access Group
    - Delete Badge
    - Delete Badge and Cardholder
    - Disable Badge
    - Replace Access Group
72. Auto Badge Management: The SMS shall allow the control and management of badge numbers within a defined pool. Once the pool of numbers is defined, the operator can automatically assign the next available number to the badge.
73. Automatic Employee IDs: The SMS shall provide a tool to define a pool of consecutive ID numbers that can be automatically assigned to each cardholder record created in the system.
74. Badge Resync: Facilities that use entry and exit terminals require cardholders to enter and exit an area in sequence. That is, when cardholders badge in at an entry terminal, they must badge out at the next badging. If, for example, they follow another cardholder out without swiping their badge, their badge will remain in the *In* state (out-of-sync). When they attempt to badge back into the area, they will be denied access. The SMS shall provide the capability of manually adjusting the state of a badge to return it to a correct state. The operator shall also be able to reconfigure the badge as Undefined to clear the Entry/Exit status until the next badging. The SMS shall allow badges to be resynced by*:*
    a. **Cardholders** – to resync the status of badges that belong to all or specific cardholders.
    b. **Last Badging Terminal** – to resync the status of all badges last presented at the selected terminal.
    c. **Last Badging Terminal Group** – to resync the status of all badges last presented at all terminals in the selected terminal group.
75. Image Recall: The SMS shall allow the system to display a cardholder's picture and information whenever he/she badges at a specific terminal or group of terminals. When a cardholder badges at a terminal under one of the following filtering conditions, the cardholder image linked to the badge number shall display, along with their name, date/time, badge number, terminal, user-defined fields, and the transaction message. The SMS shall allow the display to pop-up in front of other windows whenever a badge meets one or all of the following defined filtering criteria:
    - Access Grant
    - Access Deny
    - Invalid Card
    - Invalid Issue Level
    - Invalid PIN
    - Duress
    - Anti-Passback On
    - Invalid Card Time Zone
    - Invalid Reader
76. Manual Controls: The SMS shall allow some system functions to be operated manually from a workstation. Operators with the appropriate permissions can manually control doors, output devices, and panel relays. For example, an operator can unlock all doors at once, manually trigger an event, or allow a guard to manually control access to a specific door during off business hours.

77. Security Threat Level Alert: The SMS shall provide a rapid method of restricting access in case of an emergency. In the event of a security breach, an authorized operator shall be able to quickly change access privileges for all cardholders at any reader terminal. The default security level for these terminals is 0 (the lowest) and could be raised up to 99 (the maximum security level). The SMS shall allow configuration and control of terminal security levels by color and range. Security levels shall be mapped to a five-color "Red-Orange-Yellow-Blue-Green" system, each of which can be set a numeric value range. Users shall assign security levels to access badges. To obtain access at a door, the badge security level shall be equal to or higher than the terminal security level. When an event occurs, an operator shall raise the security level of the terminals in question and access shall be immediately restricted.
78. Area Control: The SMS shall provide a feature to control the number of cardholders that are allowed within a specific area. Operators shall be able to monitor the area at any time to determine the current number of cardholders in a particular area, and the entry and exit of personnel or vehicles into and out of a controlled area (for example, a room or parking structure). The SMS shall report and display in real time, the number and names of cardholders within the area at any given time.
79. Mustering: The SMS shall track personnel movement in the event of an emergency. During the emergency, all personnel that had logged into a risk area are expected to evacuate and are required to present their badge at a reader away from the risk area. This feature shall allow real-time printed reports and online display information to enable operators to track movement of personnel out of the risk area. This information shall be used to direct search and rescue operations. One or more areas within a plant or facility can be designated as Muster Zones.
80. Intrusion Detection: The SMS shall interface with intrusion panels to sense intrusion into a protected building. The intrusion detection system shall consist of sensors, connected to the intrusion panel, capable of detecting various intrusion or burglary events. These intrusion detection sensors shall be associated with physical points and grouped into areas. The intrusion system shall use audible annunciators to signal that an intrusion area is in alarm condition. The SMS shall be able to obtain status information whenever an intrusion component changes and shall issue commands to control the intrusion points, areas, and annunciators that are part of the intrusion system.
81. Hours on Site: The SMS shall allow operators to record a cardholder's accumulated number of hours present at a site. This feature shall be used exclusively for tracking and reporting purposes, and shall work by recording the cardholder's time interval between the time the cardholder badged in and out at reader terminals defined to monitor Hours on Site. Operators shall use any readers and define multiple areas to track cardholder time in an area. They shall be able to run a report against the areas to determine the total amount of time a badge was in.
82. Event Processing: Events are sequences of system commands or actions that shall be activated or deactivated at a pre-defined time or on an as-needed basis. The SMS shall provide tools to activate and deactivate events either manually or automatically. The SMS shall provide configuration of the following event types:
    a. **Panel Card Events**: The SMS shall allow the definition of panel card events, which are executed by a cardholder at a keypad card reader. Panel card events shall be created for a specific panel and shall operate independently from the system. If the system network shall go down for any reason, the panel card events shall continue to operate, even while the panel is offline. A panel card event is based on badge activity and shall be used to suppress or unsuppress an input group, activate or deactivate an

output group, operate a door strike, and/or reset a panel alarm relay. The panel card event shall be defined by the following parameters:

1) Alphanumeric event name
2) Panel and terminal names that shall be used to activate/deactivate the event
3) Event privilege level (0-7). This entry shall correspond to the cardholder’s privilege level, which shall be equal to or greater than the privilege level defined for the panel card event in order to initiate the event
4) Event trigger type to indicate the condition that will trigger the event (a card only, card + PIN code, card + keypad code, card + PIN + keypad code, any void card, or a special access flag)
5) Keypad code that activates or deactivates the event
6) Duration of the event execution (0-1440 minutes)
7) Input point group to be suppressed or unsuppressed
8) Output point group to be activated or deactivated
9) Door strike operation selection
10) Reset panel alarm relay selection

b. **Host Events (Triggers)**: Triggers determine what conditions must be met to initiate a specific action. The SMS shall provide the operator with a scrolling list of event triggers, which may be combined with the event logical operators listed below to program a custom sequence of events.

c. **Host Events (Actions)**: The SMS shall provide a scrolling list of event actions that shall be performed by the system when the related trigger occurs. The SMS shall allow the user to attach one or more actions to the event triggers to program a custom sequence of events..

d. **Logical Operators for Trigger Conditions**: The SMS shall provide a scrolling list of the following logical operators for event trigger conditions:

- = (Equal to)
- ! (Not equal to)
- > (Greater than)
- < (Less than)
- >= (Greater than or equal to)
- <= (Less than or equal to)

e. **Logical Operators for Triggers**: The SMS shall the provide the following event trigger logical operators to allow the user to attach one or more of the logical operators with one or more of the event triggers and actions listed above to program a custom sequence of events.

- And
- Or

83. Real-time System Activity Window: The SMS shall provide a real time system activity window to display all system transactions as they occur. The real time activity window shall display on any authorized operator workstation screen whenever the SMS server is online. This window shall have the capability to toggle the display on and off, as well as to selectively display all or the following specific transaction types:

- Panel
- Host
- Elevator
- Intrusion
- Access Deny
- Access Grant
- Area
- Intercom

- Audit
- Alarm
- Cabinet
- Badge Trace
- Guard Tour
- Mustering

a. The SMS shall provide color configuration capabilities for each of the above transaction types to help operators recognize a specific type of transaction. In addition, in transactions associated with cardholders, the real time system shall display cardholder information including entity portrait and badge transaction history. Operators shall be able to print from the workstation all or individual transactions displayed in the real time activity window.

b. The SMS shall provide remote monitoring by allowing operators to monitor transactions from multiple facilities at multiple geographical locations in real time. For transactions that have associated cameras, the SMS shall enable operators to view real time or archived audio-visual recording from any transaction or surveillance camera, from any place, at any time.

84. Real Time Maps: The SMS shall display the current status of terminals, inputs, outputs, and other defined elements on a map layout of the facility. The operator shall be able to “drag-and-drop” dynamic icons to their actual locations on layout images which shall blink to indicate the exact location of an alarm. The maps shall have the following characteristics:

a. Layout maps shall be scanned or drawn and then saved in an importable format. The SMS shall support the importing of image formats produced with any graphic drawing program such as *bmp*, *tif*, *wmf*, *jpg*, *pcx,* or *eps* format.

b. The SMS shall provide the following map types:

1) **System** – A System map shall automatically display when opening the Real Time Map. This map shall display any defined sub maps (Normal or Popup).

2) **Normal** – This is a sub map that shall be used as a Map Attachment or Popup Map Attachment on another map.

3) **Popup** – This is a sub map that shall be used as a Map Attachment or Popup Map Attachment on another map. Popup maps shall not be provided with navigation tools.

c. The map display window shall have Home, Previous and Up level buttons for rapid movement among map levels. It shall also provide map selection and size adjustment through a slider control to enlarge or reduce the view of the active map. The zooming of the map shall also be controlled with the mouse wheel or with the use of keyboard commands to enlarge or reduce the view of the active map.

d. The SMS shall provide the ability to specify text position for icons, as well as text font, size, color, and background color for icon labels and static text objects.

e. The SMS software shall be capable of storing a number of graphic maps. The quantity shall be limited by available hard disk storage space only.

f. The SMS shall allow the duplication of existing maps to assist buildings where the layout is the same throughout all floors. A master map shall be created with default information, and then used as a template to create additional maps.

g. The SMS shall provide tools to edit, import or export icons to produce custom icons for all map attachments (input, output, reader, etc.).

h. The SMS shall provide a palette that includes at a minimum, the following categories of predefined map icons:

1) **Map Attac**hment – shall indicate that lower level maps associated with the top layer map exist in the system. Operators shall attach sub maps to facility-level maps to display specific areas in a facility. Sub maps shall also contain sub maps

to add further detail. It shall be possible to add as many levels as needed. Operators shall navigate through the map layers using navigation tools. Maps shall indicate a normal or alarm state.

2) **Popup Map Attachment** – same as a map attachment but shall not provide navigation tools to other maps.
3) **Panels** – panel icons shall indicate a status of either up, down, or unknown.
4) **Input and Output Terminals** – input and output terminal icons shall indicate a status of either up, down, or unknown.
5) **Reader Terminals** – shall display the status of a reader terminal. In addition, users shall be able to open a door from the map by clicking on the reader icon. The door shall remain open for the time configured in the door terminal's access settings, and then close. When a door is opened in this manner, the map icon image for the reader shall change from a closed door to an opened door, while the door is opened, then shall revert back to a closed door image when the door closes.
6) **Input Points** – shall indicate the status of alarm input points located anywhere in the system. The input point icon shall flash, change color and the computer's internal sounder shall beep when an alarm condition exits. Users shall respond by either clicking on the icon or moving directly to the alarm queue window.
7) **Output Points** – shall indicate the status of an output point located anywhere in the system. Clicking on the icon shall set or reset the output point.
8) **Loop Tamper** – loop tamper alarm icons shall indicate a status of set, secure or unknown.
9) **Events** – event icons shall be defined to be manually activated from a map rather than by trigger conditions.
10) **Counter** – counter icons shall indicate a status of counter negative, counter positive or counter zero.
11) **Cameras** – for any icon that is associated with a camera, the user shall be able to click the camera icon to display live video. If stored videos associated with the alarm exist, the SMS shall provide the option to show alarm video or start recording.
12) **AV Dry Contact** – shall indicate the status of two-state (open/closed) input points that are physically connected to a CCTV switch and recognized by their physical address.
13) **Intercom** – shall indicate the status of an intercom station. In addition, when a call request is received for a station, the intercom icon shall flash on the map, and the user shall select to connect or disconnect the call. Also, if the intercom station is associated with outputs, the user shall be able to set or reset all outputs associated with the station.
14) **Intrusion** – shall indicate the status of intrusion areas, zones/points, annunciators, and intrusion devices. Upon intrusion activity, the map shall display the state change and the exact location of the activity. When a status changes, the associated intrusion icon starts flashing and users shall be able to, for example, arm or disarm an intrusion area or bypass an intrusion zone/point.
15) **Alarm Category** – Shall allow users to issue alarm commands (acknowledge, respond, or complete) for all SMS items that generate alarms, (such as input points or cameras) and that use the Alarm Category selected.

16) **Static Objects** – operators shall be able to place static text objects in the map to indicate for example, the name of an entire area, or a number to dial in case of emergency.

85. Database Partitioning: Multi-tenant building control shall be supported via database partitioning to restrict user access to a certain subset of records within the database, so that a user of one partition, for example, cannot add, modify, or view cardholder records of another partition. The SMS database can be divided into smaller sections that can be individually managed. Partitions shall structure what data is accessible by an individual operator, or by a group of operators. In a building with several tenants, each tenant shall be provided with their own user partition capable of controlling and monitoring their own cards, doors, alarms, etc. Building owners shall still retain overall control and shall override tenant commands if necessary. Each partition shall display to the user as a separate security system without incurring an additional cost.
86. Video Imaging and Badging Integration: The SMS shall provide enhanced security by providing visual identification of cardholders through the use of custom badge layouts, which shall be defined to include a number of elements, such as company logos, cardholder portraits, custom text, barcodes, and signatures. The captured and stored images can be viewed as part of a cardholder's data record on a workstation.
87. MIS Interface: The SMS shall provide the capability to receive cardholder information and data requests from an external database source, such as a Human Resources database. Using the MIS interface in conjunction with an external Open Database Connectivity (ODBC)-based program, the interface shall add, modify, and delete cardholders and their badges in the SMS according to data input from an external database. Both the external system and the SMS shall exchange a wide range of data between the Input and Output tables, including access groups, time zones, partition data, and even pictures. Cardholder information can also be queried using wildcards.
88. Metasys® BACnet Integration: The Johnson Controls Metasys Building Automation System is used to monitor and supervise facility controls such as heating, ventilation, and air conditioning (HVAC), lighting, and fire control systems. The SMS shall integrate with the Metasys system via a BACnet interface to allow Metasys M3 or M5 workstations to monitor and control the SMS in real time. The integration shall provide the following:
    a. Reduced Expenses – Integration of building controls and security management shall provide significant savings (e.g. lighting controls in a room are triggered by presenting a valid badge at an access control entry point).
    b. Integrated User Interface – A unified user interface shall allow a single user to monitor both the HVAC/lighting system and the SMS, thus eliminating the need for two separate users at certain, non-prime hours.
    c. Alarms and Events – M3 and M5 workstations shall receive SMS alarms and events, allowing the workstation operator to acknowledge them. During an alarm, the Metasys system shall perform a pre-defined action (e.g. the system turns on the lights to a room if a door open alarm has been reported for that area).
    d.
    e. Access Hardware and Status Information – the SMS hardware configuration and status information shall be accessed from an M3 or M5 workstation.
    f. Create Action Interlocks – The SMS software shall be configured to cause actions to occur within the Metasys system when access is granted.
    g. Door Commands and Output Points – The Metasys M3 or M5 workstation operator shall initiate a door-open command or trigger a security output point, all managed from a single seat operation.

89. Metasys$^{®}$ System Extended Architecture: The SMS shall integrate with the Metasys system, which uses Web-based technology to monitor and supervise facility controls such as heating, ventilating, and air conditioning (HVAC); lighting; and fire control system supplementary monitoring. This high level integration shall enable Metasys operators to access certain key security management features of the SMS from the Metasys Web-based user interface. The integration shall provide the following:
    a. The interface shall allow the SMS Host and Panel objects to be visible to the Metasys user. The Metasys user shall browse SMS items, view alarms and messages, send access control commands, and create interlock events.
    b. Reduced Expenses – Integration of building controls and security management shall provide significant savings (for example, lighting controls in a room are triggered by presenting a valid badge at an access control entry point).
    c. Integrated User Interface – A unified user interface shall allow a single user to monitor both the HVAC/lighting system and the SMS, thus eliminating the need for two separate users at certain non-prime hours.
    d. Alarms and Events – The Metasys operator shall receive alarms for registered SMS devices and shall be able to acknowledge, snooze, or discard the alarms. SMS Filtered History Transaction and Alarm events shall be forwarded to the Metasys event repository.
    e. Door Commands – The Metasys operator shall issue SMS door commands from the Metasys user interface. The operator shall choose to Lock or Unlock All Doors, or shall select to lock or unlock a single door by selecting a specific reader.
    f. Interlocks – Interlocks shall be defined as events generated on the SMS and result in actions on Metasys objects. Interlocks shall only be configured on the SMS and shall be unidirectional from the SMS to Metasys.
    g. A tool shall be provided to assign a graphic reference to the SMS alarms so when the SMS alarm is received and displayed by the Metasys system extended architecture, the operator can click the alarm to display the graphic item associated with the alarm and the item that caused the alarm. A Fully Qualified Reference Name (FQRN) of the graphic item shall be configured in the SMS, as defined by the Metasys system extended architecture.
90. Guard Tour: The SMS shall provide real-time monitoring of guard activities to verify and record that a guard has physically visited a facility within a specified time – reporting an early or late arrival to a designated guard tour station. The SMS shall use readers and input points to define each guard tour station. The SMS shall allow alarm configuration to report guard tour conditions and shall provide a control application to start and stop tours, and monitor their progress.
    a. Tours shall be activated automatically, by time zone or start time, or they shall be initiated manually by the operator. They shall run in forward or reverse order. The SMS shall allow configuration of up to 256 guard tours. Each tour shall have up to 16,000 station points. A maximum of three guards shall be assigned per tour.
    b. Patrol control shall be used to ensure that guards are visiting their appointed tour locations in sequence, and within the timing, as configured in the software. Selected tours shall be either randomly selected or fixed. If the guard does not visit the appointed stations as required by the tour sequence, an alarm shall be generated to alert the SMS operator that the guard may have been detained or assaulted.
91. CCTV Integration: The SMS shall provide controls to interface with approved CCTV systems to provide visual security in areas that may require real-time surveillance monitoring. The SMS software shall provide onscreen controls to operate the switches,

cameras, and monitors that are part of the CCTV system. Additionally, the system shall provide the controls to define and run the following:

a. Display images from a particular camera on a monitor.
b. Run a sequence on a monitor. A sequence is a set of programmed camera, monitor, and preset movements that run on a single monitor.
c. Use pan, tilt, and zoom controls for any selected camera. Enable focus and control iris functions; switch on wipers, washers, and lights for any given camera.
d. Activate tours to provide a programmed set of camera, monitor, and preset movements.
e. Play macros to provide a programmed set of steps that the operator can perform including any function provided by the associated switch.
f. Set or reset switch alarms to start a macro or tour associated with the switch.
g. Activate switch and camera auxiliaries to provide output control functions.
h. Run patterns, which shall be user-defined viewable camera paths with a beginning and an end.
i. Run presets, which shall define a preset camera position that may include pan, tilt, zoom, and focus adjustments.
j. The CCTV equipment connected to the SMS shall respond to event actions using the SMS events application. The operator shall define event actions that activate or stop a camera’s pattern, or define event actions that display the image from a particular camera on the monitor.

The SMS shall support at a minimum the following CCTV protocols:

Manufacturer	**Model**
American Dynamics®	AD1024, MegaPower 3200
BetaTech	Ademco® VideoBloX Switch
Geutebrück	CPX 24/8, CPX 48/8 VX 3 (ViCros III) KS 48 (ViCros II) KS 40
Panasonic®	SX850, SX650
Pelco®	CM9760, CM9740, CM6700, CM6800
Philips Burle (Bosch®)	LTC8100, 8200, 8300, 8500, 8600, 8800, 8900 series
Ultrak®	MaxPro-1000
Vicon®	VPS1300, VPS1344, V1422, VPS1466
Generic	General ASCII Protocol*

92. <u>DVR Integration (AV)</u>: The SMS shall provide integration with approved Digital Video Recording (DVR) systems. The integration shall allow authorized users to manage recording and Pan, Tilt, and Zoom (PTZ) functions of many cameras, including frame rate and resolution, from a single workstation. Depending on the DVR equipment, users shall be able to search, retrieve, and download real time or archived Audio/Video (AV) recordings from any transaction or surveillance camera, from any place, at any time. The integration shall provide the following:

a. Directly access DVR controls through an intuitive map screen; clicking an icon on the map screen shall allow users to select DVR control options.
b. Live video and playback options with audio shall be available from the alarm monitor, real-time map, or real-time list.

c. On-demand recording shall be achieved by setting up the SMS system to record specific predefined events.
d. Control of DVR recording parameters, including frame rate and image resolution shall be available from the SMS workstation.
e. The SMS shall be configured to automatically record specific predefined events and/or alarms with higher video quality to aid incident investigation and help save storage space by using lower resolution for the remaining recording times.
f. The SMS shall provide flexible query options to allow recalling video images by using a variety of query options: time and date, alarm events, camera ID, and DVR ID.
g. The selection, retrieval, and download of still pictures or video clips to the local PC shall be a simple process, after specifying the starting time/date and duration from a specific camera.
h. Shall provide scalability of the DVR integration with the SMS to allow for expansion to multiple sites using an unlimited number of cameras, to accommodate the expanding digital network needs of an organization.
i. A viewing panel shall be provided for live monitoring and switching of cameras and monitors within the SMS application.
j. Extensive alarm options shall be available through the integration with the SMS to include features such as Escalation, Acknowledgement/Response Required before Completion, Associated AV Channel, and Associated Real Time Map
k. The playback interface shall have fast forward, rewind, go to first frame, go to last frame, pause, and stop controls.

The SMS shall support at a minimum the following DVR protocols:

Manufacturer	**Protocol Version**
Genetec®	v3.4, v4.4, v4.5, and v4.6
Johnson Controls DVN 5000 series	v2.7 and v2.9
Honeywell® Rapid Eye™	v2.0.2
Milestone Xprotect™ Corporate	v2.0b and v2.0d
Nice®	v9, v10.5 with Service Pack 1, and v10.7
On-Net Surveillance Systems (OnSSI®) Ocularis	v1.1
Panasonic® WJ-ND300/WJ-ND300A	v4.30
Panasonic WJ-ND400	v1.01 and v1.31
Pelco® X-Portal DX8100	v1.0
Pelco X-Portal Endura™	v2.0
Verint® Loronix®	v4.3 and v4.4
Verint Nextiva™	v6.0
Verint SmartSight®	v3.5 build 3

93. Change Tracking (FDA Title 21 CFR Part 11 Compliance): The SMS shall provide a change tracking feature to assist facilities that may be subject to FDA Title 21, Code of Federal Regulation (CFR) Part 11 concerning electronic records and signatures. The SMS shall allow customer to define parameters to assure FDA Part 11 compliance. The following are general Part 11 requirements applicable to the SMS:

a. **Audit Trail** – The SMS shall provide valuable time-stamped reports to monitor day-to-day operator activity, such as how the hardware is controlled, when alarms are acknowledged, when cardholder records are changed, and more.

b. **Authorized Users** – The SMS software shall limit system access only to authorized individuals. Authorized users shall be identified by their unique combination of user name and password. The passwords for these individuals shall be configured to change periodically and shall have a minimum password length. Additionally, the software shall disable user access on multiple invalid logon attempts and shall provide for automatic log off due to user inactivity.

c. **Record Validation** – The SMS software shall provide a tampering tool to detect unauthorized record modifications. The SMS shall validate digital signatures, pointing out discrepancies and correcting discrepancies to ensure that records have a valid digital signature.

d. **Record Persistence** – All original records shall be saved in the SMS database, even if records are modified. The SMS shall generate detailed, time-stamped audit trails reports, assuring that all record changes maintain the original recorded information and thereby protecting all previous data.

e. **Record Retention** – Through software configuration, a system administrator shall define parameters to back up and retrieve records to ensure the availability of all records for a specified period of time.

94. Intercom Interface: The SMS server shall retrieve messages coming from approved intercom equipment and use them for event activation and distribution to P2000 workstations for the processing of intercom history messages and alarms. The SMS shall interface with Zenitel AlphaCom and Commend™ intercom systems to establish audio communication links between any two or more defined intercom stations. This interface shall provide SMS applications to control and display all intercom call requests coming from defined intercom stations. The operator shall be able to select a call request from the list and connect to any single intercom station, or to a group of stations. Additional intercom functions shall be defined for added flexibility, such as setting up a pop-up menu to display upon a call request, or trigger host actions that activate CCTV cameras. All intercom functions such as monitoring and responding shall also be available from the interactive map screen, providing immediate visual notification of system activity.

95. Enterprise Solution: The SMS shall allow a group of systems, consisting of more than one SMS server, to exchange cardholder information to create global cardholders, with access permissions over multiple sites. A system administrator shall enter the information only at the central server and the system subsequently shall synchronize the information with the other regional sites within the Enterprise system. This feature shall also enable operators to view remote alarm messaging information across the Enterprise system.

96. Web Access: The SMS shall enable users to perform various security management tasks from any Web-ready computer or tablet. This feature shall support different permission levels for each user, and requests can be approved and/or validated prior to being implemented to prevent unauthorized operations or changes to the SMS. User Authentication parameters shall be configured to set up directory services for Web Access. Rules shall be established to determine how requests are submitted. If requests require approval, pre-defined approvers shall approve or reject requests. If validation shall be required, a user with the proper permissions shall confirm the validity of the request before it can be fully processed. Web Access features shall include:

a. **Employee Management** – Web Access shall be used to manage employee data via the Web by adding, editing, or deleting cardholder records, badges, and journals. A cardholder’s In/Out status shall also be re-synchronized if out-of-sync.

b. **Visitor Requests** – Web Access shall allow adding visitors to the SMS, so that badges can be ready upon their arrival. Simply enter the appropriate visitor data into the system, assign a visitor sponsor, and enter the date and time period of the scheduled visit.

c. **Web Badging** – The Web Access computer shall be used as a badging station for capturing cardholder images (portraits and signatures), and encoding and printing cardholder badges.

d. **Contractor Requests** – This application shall send a request to change the validation period of one or more cardholder badges. The user sending this request must be assigned to the same company as the cardholder whose badge validation period will be changed.

e. **User Roles** – Administrators shall assign Web Access users to permission groups, which can keep unauthorized users from performing high-level actions, such as deleting cardholder records or rejecting requests.

f. **Request Approval and Validation** – Requests shall be configured to require approval and/or validation before they can be fully processed. An approver can approve or reject a request. A rejected request can be edited for re-submittal.

g. **Badging Activities** – Shall quickly and easily track the badge activities of cardholders. For example, when a cardholder presents a badge to a reader to enter or exit a secured area, operators shall view the record of the cardholder, the area the cardholder currently occupies (based on the location of the reader where the badge was last presented), and the date and time when the badge was presented to the reader.

h. **Guard Services** – Web Access shall be used to monitor, acknowledge and remove alarms, activate or deactivate output points (for example, turn on/off lights), and lock or unlock doors.

i. **Emergency Access Disable** – In an emergency, operators shall disable the account of a cardholder including the cardholder's badges and ability to log into Web Access.

97. Downloads: In addition to the automatic download function, the SMS shall provide a tool to manually download data to panels if there is an interruption in communication, for example when panels are offline for maintenance, or after a complete power failure or system upgrade. This function shall allow downloading of individual items or the downloading of all items at once. The download function in the SMS shall consist of:

a. A download status window to monitor the records in the download queue.

b. An option to download to disabled panels. This option shall allow items to be queued for download to panels that are offline.

c. Downloading badges with undefined entry/exit status. This option shall allow changing the entry/exit status of downloaded badges to Undefined.

d. A Smart Download Control application to define the time for downloading badges to panels when changes are made to access groups and terminal groups. The application shall also define the time for downloading cardholder and badge changes.

e. A delayed download for badges and access groups option to only perform downloads using the Smart Download application instead of performing the downloads immediately.

98. Service Startup Configuration: The SMS shall allow enabling or disabling any of the services at the start of communications, as well as set up recovery actions to take place if a service fails. If the Auto Start flag is enabled for a particular service, that service will start automatically and can be stopped or restarted using the Service Control or the Service Monitor application. If the Auto Start flag is disabled, the service will not start automatically and will not display in Service Control. By managing the SMS services, you can reduce system load by running only the required services.

99. System Status Display: The SMS shall provide a dynamic system display that graphically indicates status information of panels and associated devices configured in the system. This troubleshooting tool shall allow operators to quickly determine if panels and connected devices are communicating. If communications go down between the Server and the devices, the SMS shall report and display the known status of the devices. The SMS shall provide status information of the following components:

- Reader Terminals
- Output Terminals
- Outputs
- Mustering Zones
- Wireless Parameters
- Integration Components
- Input Terminals
- Inputs
- Otis Elevators
- Security Level Terminals
- Intrusion Items

100. Database Maintenance: The SMS shall provide functions to help customers maintain their database. The SMS shall support the following database maintenance actions:

a. **Application Engineering Import** – Imports a file from the Applications Engineering tool that provides baseline hardware configuration data for SMS.

b. **Backup Data (Append)** – Creates a backup of the SMS data without overwriting existing backups. For example, backing up data each day for an entire week will result in a single backup file containing data from each day the backup was performed.

c. **Backup Data (Overwrite)** – Creates a backup of the SMS data by overwriting existing backups. For example, backing up data each day for an entire week will result in a single backup file containing data only from the last day the backup was performed.

d. **Backup Images (Append)** – Creates a backup of the SMS images without overwriting existing backups. For example, backing up images each day for an entire week will result in a single backup file containing images from each day the backup was performed.

e. **Backup Images (Overwrite)** – Creates a backup of the SMS images by overwriting existing backups. For example, backing up images each day for an entire week will result in a single backup file containing images only from the last day the backup was performed.

f. **Calculate Digital Signature** – Validates the digital signatures, points out discrepancies, and corrects the discrepancies to ensure that records have a valid digital signature.

g. **Delete All Badges from OSI Database** – All badges will be deleted from the OSI database.

h. **Delete All Hardware from OSI Database** – All hardware will be deleted from the OSI database.

i. **Delete Expired Visitor Badges** – All visitor badges that have expired will be deleted from the database. Each visitor badge has a Visitor Validity Period (defined in Site Parameters), during which the badge is valid.

j. **Delete Selected Alarm** – Deletes the selected alarm from the database.

k. **Delete Unused Access Groups** – All unused access groups (i.e. access groups not assigned to any badge) will be deleted from the database.

l. **Delete Visitors Without Badges** – All visitors who have no assigned badges will be deleted from the database.

m. **Empty Alarms** – Removes all alarms from the alarm queue. This action will typically be performed when the queue displays alarms that cannot be secured, and thus cannot be discarded.

n. **Empty Alarms History** – All alarms in the Alarms History database table will be deleted.

o. **Empty Archive Database** – Removes the data from the Archive Database. This database is used for running reports.

p. **Empty Audit History** – Purges all audit history data from the database. The audit history data is time/date stamped records of user actions.

q. **Empty Download Queue** – Purges the actions from the Download Queue. This queue downloads data to selected panels. This function will typically be performed when a panel is no longer in use, but the queue still lists downloads for that panel.

r. **Empty Guard Tour Note** – Purges all guard tour notes from the database. The SMS can also be configured to remove these notes after a pre-determined amount of time.

s. **Empty Saved Muster Data** – Purges all of the muster data from the database. This data is normally saved to the database for evaluation once a Muster is terminated.

t. **Empty Smart Download Queue** – Purges the actions from the Smart Download Queue.

u. **Empty Transaction History** – Purges Transaction History data from the database. Transactions indicate some form of system activity. They can include such items as access requests and general system messages such as when a panel loses communication with a reader. Typically, transactions represent communication initiated at field panels and sent to the Server.

v. **FDA Backup Performed** – Informs the system that the FDA backup is archived, in accordance with company policies to meet FDA Part 11 record retention policy (available with the Change Tracking option).

w. **Kill All Reports** – Attempts to stop all database queries issued by a report. This is helpful if an operator accidentally tries to run an extreme report, such as all transaction history for the last two years.

x. **Load Archive Database from Backup** – Loads the data from the Archive Database. This database is used for running reports.

y. **Mark Secondary Tables** – Marks the starting point of FDA data for later analysis.

z. **Migrate Panel** – Changes the panel type from D6xx or S320 to a specified CK705, CK720, CK721, CK721-A panel or STI-MUX to match the new hardware installed in the field. The former panel's settings, such as associated terminals, output points, and input points, will be applied to the new panel.

aa. **Remove Access Groups from Disabled Badges** – Removes access groups from disabled badges. This in turn allows the Delete Unused Access Groups command to be used more efficiently.

bb. **Remove Expired Access Groups from Badges** – Removes from badges any access group assignment that is past its Temporary Access Period Void date.

cc. **Reset Counters to Zero** – All values in the Event Counters list will be reset to zero.

dd. **Reset Reserved Autobadge Numbers** – Resets these numbers, making them available. An available number can be assigned to a badge. A reserved autobadge number is a number that has already been assigned, but a badge has not yet been issued.

ee. **Set all Input Status to Unknown** – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

ff. **Set all Output Status to Unknown** – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

gg. **Set all Panel Status to Unknown** – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

hh. **Set all Terminal Status to Unknown** – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

ii. **Set Computer Default Language** – This task is to be used on systems operating in a foreign language, and allows changing the SMS default language for all users using this computer. This will also set the language in which the SMS services operate.

jj. **Shrink Database** – Commands SQL Server to free up space in the database. This process is normally performed automatically at various intervals.

kk. **Sync cardholder/badge active flags** – Synchronizes the cardholder/badge active flags, in case this uncommon problem occurs.

ll. **Synchronize OSI Transaction Counter** – Sets the SMS transaction counter to the last transaction currently in the OSI WAMS database. It would typically be used only if the OSI WAMS database was destroyed and recreated.

mm. **Update Database Default Strings** – This task is to be used on systems operating in a foreign language and causes all default data in the database (such as "Super User" partition, "Super User" menu permission group, default icon image set names, etc.) to be rewritten to the database in the current SMS language.

nn. **Update Preprocessed Report Archive tables** – Perform this action if you wish to run a Preprocessed report against an archived database.

oo. **Update Preprocessed Report tables** – Normally, this process occurs automatically each night. However, if the data has changed and you wish to run a Preprocessed report with current data, you may manually start this process.

pp. **Validate Digital Signature** – Ensures the integrity of all records and provides evidence when records have been altered. A digital signature verifies that the values in the columns of a record have not been modified by unauthorized users.

101. Request Queue View: The SMS shall provide a Request Queue database table that contains requests originated from external sources, such as Web Access requests. Since external requests involve adding, deleting, or modifying data in the SMS database, the Request Queue shall be designed to provide additional security measures in the request processing by checking all records before they are allowed to enter the SMS.

    a. The Request Queue shall allow operators to intercept requests for the purpose of reviewing, editing, and finally letting request data enter the SMS database system. The requests shall be packaged as XML documents and saved into the SMS Request Queue table. The Request Queue View window shall display current requests or requests that were archived in the Request Queue database table.

102. Reports: The SMS report feature shall provide access to all data in the system from entire databases to specific system transactions or configurations. Reports shall be reviewed on screen, printed, or exported into Excel spreadsheets.

    a. The SMS shall ship with the following reports:

        1) **Access Group** – Lists all terminals, terminal groups, floor groups, and door groups by access group.

        2) **Access Template** – Lists the details of all access templates created for the system.

        3) **Alarm Activity - Simple** – Lists alarm activities in a simpler format than the Alarm Activity Log report.

4) **Alarm Activity Log** – Lists all alarm activities.
5) **Alarm History** – Lists all alarm history in the system.
6) **Alarm History - Input Point** – Lists panel input point alarms and groups them by their associated terminal, followed by input point. This report allows users to see a list of alarms and state changes for the input points that are configured in the system.
7) **Alarm Instruction** – Lists all alarm instructions and associated text created for the system.
8) **Alarm Response Text** – Lists all response text created for the system.
9) **All Access Groups to Door** – Lists all access groups and the door terminals assigned to each.
10) **All Access Groups to Elevator/Cabinet** – Lists all access groups and the elevators or cabinets assigned to each.
11) **All Access Groups to Floor/Door** – Lists all access groups and the floors/doors assigned to each.
12) **All Access Groups to Floor/Door Group** – Lists all access groups and the floor/door groups assigned to each.
13) **All Access Groups to Terminal Group** – Lists all access groups and the terminal groups assigned.
14) **All Areas to Cardholder - Preprocessed** – Lists by cardholder name, all areas the cardholder can access and the terminal doors defined for the area.
15) **All Cardholders to Access Group - Preprocessed** – Lists by access group the cardholders assigned to that access group.
16) **All Cardholders to Area - Preprocessed** – Lists by area name, the cardholders and badges that have access to the area.
17) **All Cardholders to Door - Preprocessed** – Lists by door terminal all cardholders that have access to that terminal.
18) **All Cardholders to Elevator/Cabinet - Preprocessed** – Lists all cardholders and the elevators or cabinets assigned to each.
19) **All Cardholders to Floor/Door - Preprocessed** – Lists all cardholders and the floors/doors assigned to each.
20) **All Cardholders to Floor/Door Group - Preprocessed** – Lists all cardholders and the floor/door groups assigned to each.
21) **All Cardholders to Terminal Group - Preprocessed** – Lists by terminal group all cardholders that have access to that terminal group.
22) **All Cardholders to Time Zone** – Lists by time zone all cardholders assigned to that time zone.
23) **All Cardholders with Executive** – Lists the names of all cardholders with executive privileges.
24) **All Doors to Cardholder - Preprocessed** – Lists by cardholder name all doors and access groups assigned to the cardholder.
25) **All Elevator/Cabinet to Cardholder - Preprocessed** – Lists by cardholder name the elevators or cabinets assigned to the cardholder.
26) **All Floor/Door Groups to Elevator/Cabinet** – Lists by elevator or cabinet name all floor or door groups assigned to the elevator or cabinet.
27) **All Floor/Door Groups to Floor/Door** – Lists by elevator floor or cabinet door all floor or door groups assigned to the elevator floor or cabinet door.
28) **All Floors/Doors to Cardholder - Preprocessed** – Lists by cardholder name all elevator floors or cabinet doors assigned to the cardholder.

29) **All Terminal Groups to Door** – Lists by terminal group the terminals (doors) assigned to each group.
30) **Area Configuration** – Lists by area name, all configuration information entered in the Area Configuration dialog box.
31) **Area Control** – Lists the cardholders currently in the area, including the total number of cardholders for each count mode.
32) **Area Transaction** – Lists all transactions performed in the system for a specific area.
33) **Audit** – Lists by operator name the menu items selected by that operator during the date and time period selected.
34) **Auto-badge Number** – Lists the number and status of the badges that were created using the AutoBadge Management feature.
35) **AV Camera** – Lists all Audio Visual cameras and their associated configuration.
36) **AV Dry Contact** – Lists all Audio Visual Dry Contact relays and their configuration.
37) **AV Input Point to Camera** – Lists all Audio Visual Input to Camera mappings and their configuration.
38) **AV Monitor** – Lists all Audio Visual monitors and their associated configuration.
39) **AV Summary** – Lists by name all Audio Visual items defined in the CCTV/AV Configuration window.
40) **AV Switch** – Lists all Audio Visual switches and their associated configuration.
41) **Cardholder Entry–Exit Status** – Lists cardholder information, the entry/exit times, and status of the badge. This is useful to review cardholder movement throughout the facility.
42) **Cardholder Last Badge** – Locates a cardholder by last badging at a terminal (door).
43) **Cardholder Transaction History** – Lists transaction history by cardholder, including issue level and timed override parameters. You can select specific cardholder, badge number, terminal, history type, elevator or cabinet transaction, begin and end dates and times.
44) **Cardholder Transaction History - Simple** – This report is similar to the Cardholder Transaction History report, except that it is presented in a simpler format.
45) **Cardholders - Preprocessed** – Lists by cardholder all personal and system information, including badge numbers, access groups, card options, time zones, etc.
46) **Cardholders - Preprocessed - with UDF** – This report is similar to the Cardholders – Preprocessed report, except that it lists any User Defined Fields (UDFs) filled in for that cardholder. Each cardholder record will show only those UDFs that have had data entered into them from the Cardholder window. A record that contains no data in a UDF field will have no UDF entries in this report.
47) **Cardholders - Simple - Preprocessed** – This is a simplified version of the Cardholders – Preprocessed report that displays basic cardholder information.
48) **Cardholder - Simple - Preprocessed - with UDF** – This report is similar to Cardholders – Simple report plus any UDFs that have data entered.
49) **Cardholders with Web Access - Preprocessed** – Lists the cardholders that are assigned with menu permissions to perform Web Access functions.
50) **Cardholders without Badges** – Finds all cardholders in the system without badges assigned.

51) **CCTV Camera** – Lists all CCTV cameras and their associated configuration.
52) **CCTV Monitor** – Lists all CCTV monitors and their associated configuration.
53) **CCTV Summary** – Lists by name all CCTV items defined in the CCTV/AV Configuration window.
54) **CCTV Switch** – Lists all CCTV switches and their associated configuration.
55) **Disabled Cardholders and Badges** – Lists all cardholders that have been disabled or have disabled/inactive badges.
56) **Elevator/Cabinet Configuration** – Lists by elevator or cabinet name all configuration information entered in the Elevator or Cabinet Configuration dialog box for all elevators or cabinets; specific elevator or cabinet and panel name can be selected to limit the data.
57) **Elevator/Cabinet Transaction** – Lists all transactions performed in the system for the specified elevator or cabinet name.
58) **Enable Code** – Lists by panel name (for D600 AP panels only), the Enable Codes used at the facility.
59) **Events** – Lists by event name all configuration information entered in the Configure Events dialog box, including event trigger and action information.
60) **Floor/Door Group** – Lists all elevator or cabinet floor/door groups and the floor/door masks assigned to each group.
61) **Floor/Door Mask** – Lists all elevator or cabinet floor/door masks and the floors/doors assigned to each.
62) **Floor/Door Name** – Lists all elevator or cabinet floor/doors and the floor/door numbers and names assigned to each.
63) **Hardware Up/Down Status** – Lists the name and status of all operating hardware.
64) **Holiday** – List all holidays configured for the system.
65) **Hours on Site** – Lists a detailed report of a cardholder's accumulated number of hours present at a site.
66) **Hours on Site -** Simple – Lists a summary report of a cardholder's accumulated number of hours present at a site.
67) **Input Group** – Lists by input group the associated input points and panels.
68) **Input Point** – Lists by input point all configuration information entered in the Input Point dialog box for all input points.
69) **Input Point Disable/Suppressible** – Lists all input points in the system that are disabled or suppressed.
70) **Loop Configuration** – Lists by loop number all loop configuration information entered in the Loop Configuration dialog box for all loops.
71) **Message Filter** – Lists by message filter name all the filtering information entered in the Message Filter Configuration dialog box for all message filters.
72) **Message Filter Group** – Lists by message filter group the message filters associated with the message filter group.
73) **Message Forwarding** – Lists the workstation names "From" where and "To" where all current messages are forwarded.
74) **Muster Analysis** – Displays by group type the list of personnel who are within a Muster Zone in the specified time frame, and whether it was a drill or real emergency.
75) **Mustering Configuration** – Lists by Muster Zone name, the zone definition configuration, as set up in the Muster Zone Definition dialog box.
76) **Operator** – Lists all operator information entered in the Edit Operator dialog box.

77) **Operator Permissions** – Lists the permissions assigned to each operator.

78) **Output Group** – Lists by output group the associated output points and panels.

79) **Output Point** – Lists by output point all configuration information entered in the Output Point dialog box for all output points.

80) **P900 Counter** – Lists all counter information, as set up in the P900 Counters dialog box.

81) **P900 Flag** – Lists all flag information, as set up in the P900 Flags dialog box.

82) **P900 System Parameters** – Lists the details of the P900 parameters, as set up in the P900 System Parameters dialog box.

83) **P900 Trigger Event** – Lists all trigger event information, as set up in the P900 Trigger Event dialog box.

84) **P900 Trigger Link** – Lists all trigger link information, as set up in the P900 Trigger Links dialog box.

85) **Panel** – Lists all panels in the system with their associated configuration as set up in the Panel dialog box.

86) **Panel Card Event** – Lists by panel card event name all panel card event details configured for the system.

87) **Remote Server** – Lists all remote servers in the system with their associated configuration, as set up in the Remote Server dialog box.

88) **Security Level Ranges** – Lists the security levels defined in the Security Level Range Editor dialog box.

89) **Site Parameters** – Lists the details of the current site parameters as set up in System Configuration.

90) **Station** – Lists by workstation all workstation configurations.

91) **Terminal** – Lists by terminal name all terminal configurations as set up in the Terminal dialog box.

92) **Terminal Groups** – Lists by terminal group the terminals associated with the terminal group.

93) **Terminal Unshunted** – Lists all terminals with a shunt time of zero.

94) **Time Zone** – Lists all Time Zones configured for the system.

95) **Tour Configuration** – Lists by tour name, all tour definition configurations, as set up in the Guard Tour Definition window.

96) **Tour Notes** – Lists all the tour notes assigned to a specific tour name, as set up in the Guard Tour Control window.

97) **Tour Transaction History** – Lists all tour transactions performed in the system.

98) **Transaction History** – Lists all transactions performed in the system or can be filtered to list by specific Site, Partition (if any), transaction type (Host, Panel, Terminal, Input and Output) and history type. The history type available for selection depends on the transaction type selected.

99) **Unused Active Badges** – Displays a list of active badges that have not been used during the specified period of time.

100) **Verification** – Allows for a verification of the commissioning process by providing a list of all hardware to be checked off by the contractor. This list includes a list of all panels in the system and their associated terminals, inputs, and outputs.

b. The SMS shall fully integrate with a dynamic report writer module allowing users to create custom reports. The dynamic report writer shall be SAP® Crystal Reports® with the following features**:**

1) Mouse-driven graphical user interface with the ability to select from a list of database fields.

2) User-definable reports that can be saved and re-run as required, without redefining the report fields and format each time the report is run.

2.4 SMS HARDWARE

A. SMS Server: The minimum system server requirements shall be a standard name brand personal computer with sufficient capacity for the intended purpose. The server computer shall ship factory configured with all software pre-loaded and tested. All computer hardware replacement components shall be available from multiple third party sources. Unless otherwise approved by the manufacturer, the minimum configuration for the server shall be as defined below for a system capacity of five workstations, 128 readers and 15,000 cards:

1. Processor: Dual Core CPU
2. Memory: 4 GB
3. Video Card: 24-bit color or more
4. Monitor Size: 19” flat panel monitor
5. Storage Size: 100 GB 7200 RPM 4 MB cache Hard Disk
6. One Network Interface (10Base-T or faster)
7. Optical Drive: DVD-ROM
8. Mouse: Two-button mouse
9. Keyboard: 101-type keyboard

B. SMS Workstation: The recommended workstation requirements shall be a standard name brand personal computer with sufficient capacity for the intended purpose. The workstation shall ship factory configured with all software pre-loaded and tested. All computer hardware replacement components shall be available from multiple third-party sources. Minimum configuration for the workstation shall be:

1. Processor: Dual Core CPU
2. Memory: 2 GB
3. Video Card: 1280 x 1024 resolution, 32-bit color, 3D accelerator
4. Monitor Size: 19” flat panel monitor
5. Storage Size: 70 GB
6. Network Controller Card: 10/100 Base-T
7. Optical Drive: DVD-ROM
8. Mouse: Two-button mouse
9. Keyboard: 101-type keyboard

C. System Printer: System printers shall be provided in the quantities specified or as shown on the drawings. Printers shall be dot matrix, 180 characters per second, bi-directional printers.

D. Peer-to-Peer Network Controller (Johnson Controls)

1. .Functional Capabilities
   a. The controller shall communicate with the server over 10/100Base-T Ethernet.
   b. Should the controllers lose communication with the server, the controllers shall continue to control access and monitor change of status for all connected points. Local history of all transactions shall be buffered at the controller and automatically

uploaded to the server for alarm reporting and long-term historical storage once communications is re-established.

c. Each controller shall support up to a maximum of 64 field devices.
d. Each controller shall allow the user to:
    1) Add modules to connect readers
    2) Monitor 2 or 4-state input points
    3) Add output relays to perform manual or automatic control functions
    4) Link input points to output relays

2. Technical Specification
    a. The controller shall have the following input power requirements: min. 20VDC, nominal 24V, max. 30VDC, max. 1A.
    b. The controller shall require ambient operating temperature from 32 to 122 °F (0 to 50° C) with a relative humidity of 10 to 85% non-condensing.
    c. Each controller shall incorporate the following components:
        1) Embedded 32-bit processor.
        2) 128 MB onboard flash memory (for the operating system and database).
        3) 3V lithium battery.
        4) IN1 and IN2 binary inputs, unsupervised.
        5) Binary output – Form C Relay, SPDT, 24VDC maximum.
        6) LED indicators (POWER, FAULT, RS485 A, RS485 B, ETHERNET, 10/LINK, 100/LINK, and RUN).
        7) Connectors:
            a) RS232 A – RS-232 Serial Interface
            b) DB9 port for the user interface to workstations or laptop computers
            c) RS232 B – RS-232 Serial Interface, dual use: transaction logger port or KONE elevator controller communications port
            d) RS485A – OTIS BMS elevator communication
            e) RS485B – For field device communication
            f) RJ45 – 10/100Base-T network port for host communication
    d. Certifications: FCC Part 15 Class B, CE Mark, C-Tick, UL 294 and UL 1076.
3. Software Features
    a. The controller shall provide the following software features:
        1) Support for encryption between controller and the host.
        2) Up to 64 readers per controller.
        3) Up to 12 facility codes per reader (192 per controller).
        4) Up to 40 holidays.
        5) Up to 64 time zones.
        6) Elevator integration.
        7) Support for Wiegand, smart card, proximity, magnetic strip, barium ferrite, most biometric readers and bar code card technologies.
        8) Support for custom engineered formats.
        9) Accepts badge numbers of up to 20 digits.
        10) Supports up to 8 access group / time zone pairs per badge.
        11) Storage capacity for up to 120,000 cardholders.
    b. The controller shall provide the following system features:
        1) Expandable modular design – User shall be able to connect multiple controllers via Ethernet for a total system capacity of 2,048 doors. .
        2) Easy integration with the server - All controllers shall be connected to, programmed, and monitored via the server.

E. Two-Door Interface Module (Johnson Controls)

1. Functional Capabilities
   a. The two-door interface module shall use RS-485 bus communications with the network controller, 2 or 3-wire.
   b. The two-door interface module shall support 9600/19200 auto baud rate detection.
   c. The two-door interface module shall provide the following I/O interfaces:
      1) Supervised door monitor switch input, normally open or normally closed, based on wired configuration.
      2) Supervised auxiliary access or exit request switch input, normally open.
      3) Supervised tamper and spare inputs.
      4) Wiegand Data0 and Data1 interface.
      5) Door strike relay, SPDT.
      6) Alarm shunt relay, SPDT.
      7) Red lamp driver and green lamp driver (open collectors).
   d. The following inputs shall be shared by all interfaces (one per module):
      1) Calibration resistor input.
      2) Supervised panel tamper and power fail inputs.
   e. The two-door interface module shall allow for reader terminal I/O points to be re-assigned from reader-specific functions to general purpose I/O points.
2. Technical Specification
   a. The two-door interface module shall have the following power requirements:
      1) Input voltage: +12 to 24VDC, 16 to 24VAC
      2) Input current: 1A at 24V, 2A at 12V
      3) Power: 24W
   b. The two-door interface module shall require ambient temperature from 32º to 122ºF (0º to 50ºC).
   c. The two-door interface module shall require humidity from 10 to 85% non-condensing.
   d. Relay outputs shall require 1A max. 0-24 VDC/VAC, 25VA maximum.
   e. Red LED/Green LED outputs shall require 50mA maximum 0-24VDC.
   f. The two-door interface module shall provide 250mA at 12VDC for each reader.
   g. Certifications: FCC Part 15 Class B, CE Mark, C-Tick, UL 294 and UL 1076.

F. 8-Door Interface Module (Johnson Controls)

1. Functional Capabilities
   a. The 8-door interface module shall use RS-485 bus communications with the network controller.
   b. The 8-door interface module shall support 9600/19200 auto baud rate detection.
   c. The 8-door interface module shall provide the following I/O interfaces:
      1) Supervised door monitor switch input, normally open or normally closed, based on wired configuration.
      2) Supervised auxiliary access or exit request switch input, normally open.
      3) Supervised tamper and spare inputs.
      4) Wiegand Data0 and Data1 interface.
      5) Door strike relay, SPDT.
      6) Alarm shunt relay, SPDT.
      7) Red lamp driver and green lamp driver (open collectors).
      8) +12VDC 250mA reader power supply.

d. The following inputs shall be shared by all interfaces (one per module):
   1) Calibration resistor input.
   2) Supervised panel tamper and power fail inputs.

e. The 8-door interface module shall allow for reader terminal I/O points to be re-assigned from reader-specific functions to general purpose I/O points.

2. Technical Specification
   a. The 8-door interface module shall have the following power requirements: nominal voltage +12 to +24VDC, min. +10.8, max. +30VDC, 48W.
   b. The 8-door interface module shall require ambient temperature from 32º to 122ºF (0º to 50ºC).
   c. The 8-door interface module shall require humidity from 10 to 85% non-condensing.
   d. Relay outputs shall require 1A max. 0-24 VDC/VAC, 25VA maximum.
   e. Red LED/Green LED outputs shall require 1000mA maximum 0-24VDC.
   f. The two-door interface module shall provide 250mA at 12VDC for each reader.
   g. Certifications: FCC Part 15 Class B, CE Mark, C-Tick, UL 294 and UL 1076.

G. Input/Output Interface Modules (Johnson Controls)

1. Functional Capabilities
   a. The I/O interface modules shall use RS-485 bus communications with the network controller.
   b. The I/O interface modules shall support 9600/19200 auto baud rate detection.
   c. Each 32IO16 interface module shall have 8 input/output terminals, and each terminal shall include:
      1) 4 supervised inputs (4-state).
      2) 2 relay outputs.
      3) 2 open collector outputs (OUT1 and OUT2).
   d. Each I16 module shall have 16 inputs (2-state).
   e. Each SIO8 module shall have 8 supervised inputs (4-state) and 8 outputs.
   f. Each IO8 module shall have 8 inputs (2-state) and 8 outputs.
   g. Each SI8 module shall have 8 supervised (4-state) inputs.
   h. The following inputs shall be shared by all interfaces (one per module):
      1) Calibration resistor input.
      2) Supervised panel tamper and power fail inputs.
2. Technical Specification
   1) The I/O interface module shall have the following power requirements: nominal voltage +12 to +24VDC, min. +10.8, max. +30VDC, 48W.
   2) The I/O interface module shall require ambient temperature from 32º to 122ºF (0º to 50ºC).
   3) The I/O interface module shall require humidity from 10 to 85% non-condensing.
   4) Relay outputs shall require 1A max. 0-24 VDC/VAC, 25VA maximum.
   5) OUT1/OUT2 outputs shall require 1000mA maximum 0-24VDC.

PART 3 – EXECUTION

3.1 EXAMINATION

A. Examine the areas and conditions where SMS equipment is to be installed and notify the Owner's Representative of conditions detrimental to the proper and timely completion of the work.

B. Do not proceed with the work until unsatisfactory conditions have been corrected in a manner acceptable to the Owner's Representative.

3.2 INSTALLATION

A. ACS components shall be mounted and interconnected in accordance with equipment manufacturer's written instructions, in compliance with NFPA 70 and ANSI C2 and with recognized industry practices, to ensure that the ACS complies with all requirements stated herein and serves its intended purposes.

B. Installation shall also comply with Owner's site-specific requirements as noted in the Contract Documents.

C. Wiring Method: Install wiring in metal raceways [except in accessible indoor ceiling spaces and in interior hollow gypsum board partitions where cable may be used]. Conceal raceways and wiring except in unfinished spaces and as indicated. Minimum conduit size shall be 1/2-inch. Control and data transmission wiring shall not share conduit with other building wiring systems. Install junction boxes where required for SMS equipment.

D. Surface-mounted equipment shall be securely fastened to structural supports. Ensure that this equipment is plumb and level.

E. Connectors and terminals, including screws and bolts, shall be tightened in accordance with equipment manufacturer's published torque tightening values. Where manufacturer's torquing requirements are not indicated, tighten connectors and terminals to comply with the tightening torques specified in NFPA 70.

F. Equipment grounding connections for SMS components shall be provided. Ground connections shall be tightened to comply with the tightening torques specified in NFPA 70 to assure permanent and effective grounds. Grounding equipment shall comply with UL 467.

G. Coordinate AC wiring requirements and electrical characteristics with site electrical system for operation with normal power and backup power sources.

3.3 FIELD QUALITY CONTROL

A. Repair any damages done to the facility or its contents caused during the work. Repairs shall be performed as quickly as possible after the damage occurs. Repairs must be made in a professional manner and are subject to inspection and acceptance by the Owner's Representative.

B. Touch-up scratched and marred surfaces to match the original finishes.

3.4 ADJUSTING

A. Upon completion of installation of SMS components, set all field-adjustable controls and components and align and calibrate all equipment for the required performance and operation as specified herein.

3.5 DEMONSTRATION

A. The Contractor shall be responsible for testing and commissioning the SMS installation in accordance with all applicable documents in the Contract set.

1. Testing shall be comprehensive and sufficient to demonstrate compliance with each requirement.
2. Prior to energization, all field-run wires and cables shall be tested for electrical continuity and short circuits and to ensure proper polarity of all connections.

B. A proposed test plan shall be submitted to the Owner’s Representative for approval before commencement of final acceptance test.

C. Final acceptance tests shall be conducted in the presence of the Owner’s Representative.

D. During the final acceptance tests, malfunctioning components shall be corrected at the site where possible; otherwise, the Contractor shall remove and replace. Upon correction or replacement, the component shall be retested.

3.6 TRAINING

A. Operator training shall consist of a two-day course conducted on-site by a factory trained professional instructor. Training conducted by unqualified personnel is unacceptable.

B. Training materials shall consist of the following:

1. Formal course outline and agenda.
2. Operator training student guide for each student.
3. Hands-on practice with online equipment.
4. Written examinations.

C. The training course shall be for at least two continuous business days.

D. Additional video imaging training sessions shall be made available to the Owner if necessary, at additional cost.

END OF SECTION